ETÄYHTEYSRATKAISUN TOTEUTTAMINEN JA TUOTTEISTAMINEN

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2009
Tony Voutilainen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

TONY VOUTILAINEN: Etäyhteysratkaisun toteuttaminen ja tuotteistaminen

Tietoliikennetekniikan opinnäytetyö, 56 sivua, 3 liitesivua

Kevät 2009

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on etäyhteysratkaisun toteuttaminen ja tuotteistaminen. Tavoitteena on suunnitella, toteuttaa ja tuotteistaa etäyhteysratkaisu Lahti Precision Oy:lle. Toimiva ja hyvin toteutettu etäyhteysratkaisu tuo yritykselle huomattavia säästöjä, kun asiantuntijainsinöörien ei tarvitse matkustaa ongelmatilanteissa asiakkaiden luokse. Myös vasteajat ongelmatilanteissa pienenevät huomattavasti. Tuotteistettu etäyhteysratkaisu on yrityksen kannalta helpompi toteuttaa ja myydä asiakkaalle.

Opinnäytetyössä tutustutaan erilaisiin VPN-menetelmiin ja tarkastellaan niiden sopivuutta yrityksen käyttöön. VPN-yhteydet voidaan hankkia ulkoistettuna palveluna tai toteuttaa itse ohjelmisto- tai laitteistopohjaisena. Laitevertailut ja -testit ovat tärkeässä osassa tätä opinnäytetyötä, sillä tavoitteena oli löytää luotettava, turvallinen ja samalla kustannustehokas laiteratkaisu etäyhteyksien toteuttamiseen.

Testeissä valittua laiteratkaisua testattiin pilottihankkeella Lahti Precision Oy:n ja Turkissa sijaitsevan asiakastehtaan välillä. Pilottihankkeesta saatiin arvokasta tietoa ja kokemusta etäyhteysratkaisun tulevia toteutuksia varten. Toinen etäyhteys tehtiin Lahti Precision Oy:n ja Ukrainassa sijaitsevan asiakastehtaan välillä. Tässä hankkeessa etäyhteys toteutettiin lopullisessa ratkaisussa käytettävän laiteparin välillä.

Etäyhteysratkaisun tuotteistamisessa keskeisessä osassa ovat asiakkaille ja yrityksen henkilökunnalle tehtävät dokumentit. Näitä dokumentteja ovat mm. esite, tekninen palvelukuvaus ja konfigurointiohje. Dokumenttien avulla Lahti Precision Oy:n on helppo saada aikaan keskustelua asiakkaan kanssa etäyhteyksien mahdollisuuksista ja yrityksen työntekijöillä on valmiudet toteuttaa etäyhteysratkaisuja. Tuotteistamiseen kuului myös työntekijöiden koulutus.

Opinnäytetyöprojekti onnistui tavoitteessaan luoda toimiva ja tuotteistettu etäyhteysratkaisu. Etäyhteydet ovat jo olleet työntekijöiden käytössä ja tulevaisuudessa käyttöaste kasvaa, kun asiakastehtaiden määrä nousee. Etäyhteysratkaisu maksaa itsensä yritykselle nopeasti takaisin, kun työntekijöiden matkustustarve vähenee.

Avainsanat: etäyhteys, etätuki, VPN, SSL, tuotteistaminen

Lahti University of Applied Sciences
Degree Programme in Information Technology

VOUTILAINEN, TONY: Implementation and productization of remote access solution

Bachelor´s Thesis in Telecommunications Technology, 56 pages, 3 appendixes

Spring 2009

ABSTRACT

The subject of this thesis is the implementation and productization of a remote access solution. The objective was to plan, implement and productize a remote access solution for Lahti Precision Ltd. A functional and well implemented remote access solution will bring significant savings for the corporation since it will become unnecessary to dispatch experts to the customer locations when problems occur. Response times will also be positively affected. A productized remote support solution is also easier to implement and sell to the customer.

The thesis introduces various VPN methods and reviews their suitability for the corporation. Hardware comparison and testing are an important part of the thesis, since the objective was to find a reliable, safe and cost efficient hardware solution for the remote access implementation.

The chosen hardware setup was put to a test in a pilot project between Lahti Precision Ltd. and a customer factory located in Turkey. The project provided valuable information and experience for future remote access solution implementations. A second remote access solution was implemented between Lahti Precision Ltd. and a customer factory located in Ukraine. In the second project the remote access solution was implemented between a device pair which was used in the final solution.

The documentation created for customers and the corporation’s staff is an essential part of productizating a remote access solution. Such documents include a brochure, a technical service description and a configuration manual to mention but a few. Using the documentation it will be easy for Lahti Precision Ltd. to engage in conversations with the customers about the possibilities of remote access and the staff will have the means to implement various remote access solutions. Staff training was also included in the productization process.

The thesis project succeeded in its objective to create a functional and productized remote access solution. The remote access has already been in use by the staff and the usage will grow in the future as the number of customer factories rises. The remote access solution will pay itself back in a short period of time as the staff’s need for travel decreases.

Keywords: remote access, remote support, VPN, SSL, productization

SISÄLLYS

LYHENNELUETTELO

3DES	Triple-DES, lohkosalausmenetelmä, kts. DES
ad hoc	tiettyyn tarkoitukseen kehitetty menetelmä
AES	Advanced Encryption Standard, lohkosalausmenetelmä
AH	Authentication Header, autentikointiotsake, IPsec:in pakettivirtojen suojaamiseen käyttämä protokolla
ALG	Application Level Gateway, sovellustason yhdyskäytävä
AT&T	Yhdysvaltalainen puhelinoperaattori
ATM	Asynchronous Transfer Mode, asynkroninen tiedonsiirtotapa
CHAP	Challenge Handshake Authentication Protocol, kolmisuuntainen kättely-yhteyskäytäntö
DES	Data Encryption Standard, lohkosalausmenetelmä
DH	Diffie-Hellman, VPN-autentikoinnissa käytetty salausmenetelmä
ESP	Encapsulating Security Payload, IPsec:in pakettivirtojen suojaamiseen käyttämä protokolla
FQDN	Fully Qualified Domain Name, täydellinen toimialuenimi
FTP	File Transfer Protocol, tiedonsiirtomenetelmä
GRE	Generic Routing Encapsulation, Ciscon kehittämä IP-tunnelointiprotokolla

H.323	signalointiprotokolla
ICMP	Internet Control Message Protocol, TCP/IP-pinon kontrolliprotokolla
ICV	Integrity Check Value, kehyksen tarkistussumma
IETF	Internet Engineering Task Force, Intenet-protokollien standardoinnista vastaava organisaatio
IKE	Internet Key Exchance, IPsec-protokollan avaintenvaihtoon tarkoitettu sovellus, kts. ISAKMP, Oakley ja SKEME
IP	Internet Protocol
IPsec	IP Security Architecture, joukko TCP/IP-pinoon kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen
IPv4	IP-protokollan neljäs versio
IPv6	IP-protokollan kuudes versio
ISAKMP	Internet Security Association and Key Management Protocol, avaintenhallintaprotokolla
L2F	Layer 2 Forwarding, Ciscon kehittämä VPN-protokolla
L2TP	Layer 2 Tunneling Protocol, Ciscon ja Microsoftin kehittämä VPN-tunnelointiprotokolla
LAC	L2TP Access Concentrator, L2TP-tunnelin luova yhdistäjälaite

LNS	L2TP Network Server, L2TP-tunnelin luonnin vastaantottava osapuoli
MD5	Message-Digest algorithm 5, kryptografinen tiivistefunktio
NAPT	Network Address Port Translation, osoitteen- ja portinmuunnos
NAS	Network Access Server, yhdyskäytävänä toimiva palvelin
NAT	Network Address Translation, osoitteenmuunnos
NAT-OA	NAT Original Address
NAT-T	NAT Traversal
Oakley	määrittelee avaintenvaihdon tilat
OSI	Open Systems Interconnection, OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa, vrt. TCP/IP
PPP	Point-to-Point Protocol, yhteysprotokolla
PPTP	Point-to-Point Tunneling Protocol, PPP-protokollaan pohjautuva VPN-tunnelointimenetelmä
PSK	Pre-Shared Key, ennalta jaettu salausavain
RAS	Remote Access Server, verkkoon pääsyä välittävä palvelin
RFC	Request for Comments, IETF-organisaation julkaisemia Internetiä koskevia standardeja

SA	Security Association, määrittelee IPsec-tunnelin osapuolien väliset salausasetukset
SHA-1	Secure Hash Algorithm-1, kryptografinen tiivistefunktio
SIP	Session Initiation Protocol, VoIP-yhteyksien luonnista vastaava tietoliikenneprotokolla
SKEME	määrittelee mukautuvan avaintenvaihtotekniikan
SPI	Security Parameters Index, 32-bittinen yhteystunnus
SSH	Secure Shell, turvalliseen tiedonsiirtoon tarkoitettu järjestelmä
SSL	Secure Sockets Layer, salsusprotokolla, kts. TLS
TCP	Transmission Control Protocol, yhteydellinen viestinvälitysprotokolla
TCP/IP	Transmission Control Protocol / Internet Protocol, Internet-liikennöinnissä käytettävien tietoverkkoprotokollien yhdistelmä, TCP/IP-malli kuvaa tiedonsiirtoprotokollien yhdistelmän neljässä kerroksessa, vrt. OSI
TLS	Transport Layer Security, salausprotokolla, aiemmin tunnettu nimellä SSL
UDP	User Datagram Protocol, yhteydetön viestinvälitysprotokolla
userID	käyttäjätunnus tai -tunniste
VPN	Virtual Private Network, virtuaalinen yksityisverkko

X.509 standardi, joka määrittelee varmenteen ja varmenteita käyttäviä autentikointiprotokollia

1 JOHDANTO

Etäyhteyksien toteuttamiseen on tarjolla monia eri vaihtoehtoja ja ratkaisuja. Tietoturvallisuus on erittäin tärkeää ottaa huomioon etäyhteyksien yhteydessä, sillä etäyhteydet kulkevat julkisten verkkojen läpi. Yleisesti etäyhteyksien toteuttamiseen käytetään virtuaalisia yksityisverkkoja eli VPN:ää, jolla saadaan muodostettua turvallinen siirtoyhteys julkisen tiedonsiirtokanavan yli. VPN-yhteyksien avulla yritykset voivat toimia tehokkaasti asiakkaidensa ja yhteistyökumppaniensa kanssa eri puolilla maailmaa säilyttäen samalla vaadittavan tietoturvatason.

VPN-yhteydet voidaan toteuttaa ohjelmisto- tai laitteistopohjaisesti. Ohjelmistopohjaisissa ratkaisuissa käytetään VPN-asiakasohjelmistoja. VPN-asiakasohjelmistoja käyttävät yleensä paljon liikkuvat työntekijät, joiden on tärkeää saada etäyhteys paikasta riippumatta. Laitteistopohjaiset ratkaisut ovat kiinteitä ja niitä käytetään yhdistämään kaukana toisistaan olevat sisäverkot.

Opinnäytetyön teoriaosuudessa tutustutaan yleisesti VPN:ään ja yleisimpiin VPN-topologioihin. VPN-tunnelointiprotokollista IPsec on laajin osa opinnäytetyöprojektia. IPsecin alla tutustutaan sen käyttämiin salausmenetelmiin ja yleiseen toimintaan. Myös muita yleisimpiä tunnelointiprotokollia käydään läpi ja suoritetaan protokollien välinen vertailu.

Opinnäytetyön kohdeyrityksenä oli Lahti Precision Oy. Opinnäytetyöprojektin tavoitteena oli suunnitella, toteuttaa ja tuotteistaa kustannustehokas etäyhteysratkaisu. Opinnäytetyön jälkimmäisessä osuudessa käydään läpi etäyhteysratkaisulle asetetut vaatimukset, tehdyt laitevertailut- ja testit sekä toteutetut etäyhteydet. Toimivan etäyhteysratkaisun avulla kohdeyritys voi olla yhteydessä ympäri maailmaa sijaitseviin asiakastehtaisiin turvallisesti ja käytännöllisesti.

2 VIRTUAALISET YKSITYISVERKOT (VIRTUAL PRIVATE NETWORK, VPN)

2.1 Taustaa ja yleistä tietoa VPN:stä

VPN terminä juontaa juurensa puhelinverkkojen aikaan. VPN kuvasi alunperin yksityisten puhelinvaihteiden välisiä yhteyksiä julkisissa puhelinverkoissa. Puhelinyhtiöt alkoivat käyttämään julkisia puhelinverkkoja yksityisen kommunikaation helpottamiseksi, minkä johdosta puhelinyhtiöiden asiakkaat pystyivät laajentamaan yksityisiä puhelinverkkojaan. Tähän aikaan puhuttiin vielä puhe-VPN:stä (Voice VPN). Puhe-VPN sai alkunsa Yhdysvalloista, jossa puhelinyhtiöt kilpailivat 1980-luvulla kaukoyhteyksien tarjoamisesta. AT&T (American Telephone and Telegraph) kehitti menetelmän, jolla pystyttiin muuttamaan puhelinvaihteissa käytettyjen ohjelmien asetuksia; toimipaikkojen yksityiset numerot korvattiin yrityksen julkisilla numeroilla jokaisessa yrityksen toimipisteessä. (Perlmutter & Zarkower 2001, 30.)

VPN:n avulla voidaan muodostaa näennäisiä yksityisiä verkkoja julkisen verkon, kuten internetin yli. Verkkoja kutsutaan virtuaalisiksi, koska ne perustuvat virtuaaliyhteyksiin. Yhteydet ovat siis väliaikaisia, eivätkä ole fyysisesti olemassa; paketit reititetään julkisessa verkossa laitteiden välillä ad hoc –mallin mukaisesti. VPN siis luo salatun, suljetun ja luotettavan siirtotien julkisen verkon yli. VPN-yhteys muodostetaan joko kahden laitteen, laitteen ja verkon tai kahden verkon välille. Virtuaalisten verkkojen palvelut ja resurssit ovat vain niihin oikeutettujen käyttäjien käytettävissä. (Scott, Wolfe & Erwin 1999.)

VPN voidaan toteuttaa joko ohjelmisto- tai laitteistopohjaisena tai yhdistämällä molempia. Ohjelmistopohjainen VPN käyttää niinkutsuttuja asiakasohjelmistoja (VPN client), jotka esiasennetaan työasemaan. Ohjelmistopohjainen ratkaisu on yleensä käytössä, kun yksittäinen käyttäjä haluaa ottaa VPN-yhteyden muualla olevaan yksittäiseen isäntään tai yksityiseen verkkoon. Yksittäisessä

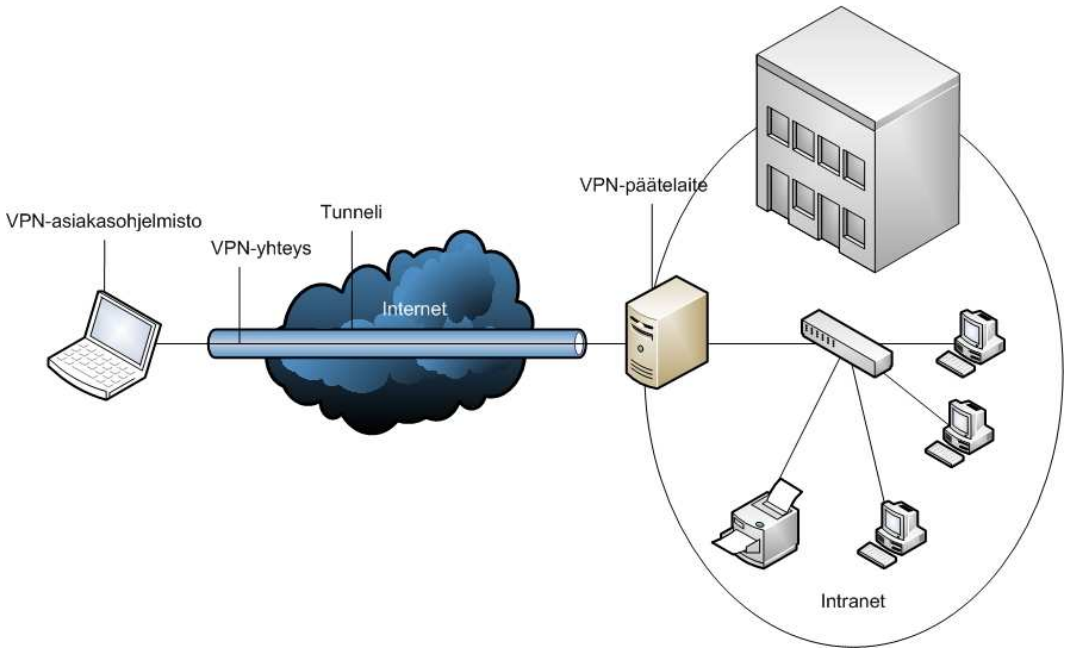
isäntäkoneessa riittää asiakasohjelmisto, mutta yksityisen verkon päässä täytyy olla jokin VPN-laite. Kokonaan laitteistopohjaiset ratkaisut toteutetaan niihin tarkoitetuilla tietoliikennelaitteilla, joita ovat mm. reitittimet, palomuurit ja palvelimet. Tämä ratkaisu on yleensä käytössä, kun VPN:llä yhdistetään kaksi yksityistä verkkoa. (Viestintävirasto 2007c.)

2.2 Käyttötarkoitukset

VPN:n avulla henkilö tai yritys voi kasvattaa informaation saatavuutta huomattavasti. Etenkin yritysmaailmassa tiedon saatavuuden lisääminen on huomattava etu sekä yrityksen työntekijöille että yhteistyökumppaneille. VPN mahdollistaa työntekijöille etätyön tietoturvallisella tavalla. Turvallisuus onkin tiedon saatavuuden lisäksi toinen VPN:n kulmakivistä. Koska tiedon saatavuus kasvaa, ja siihen mahdollistetaan pääsy julkisista verkoista, täytyy tietoturvaan kiinnittää enemmän huomiota. Kyseessä on kuitenkin yksityinen verkko, kuten esimerkiksi yrityksen intranet, joten luvattomat käyttäjät halutaan varmasti pitää verkon ulkopuolella edelleenkin. (Scott, Wolfe & Erwin 1999.)

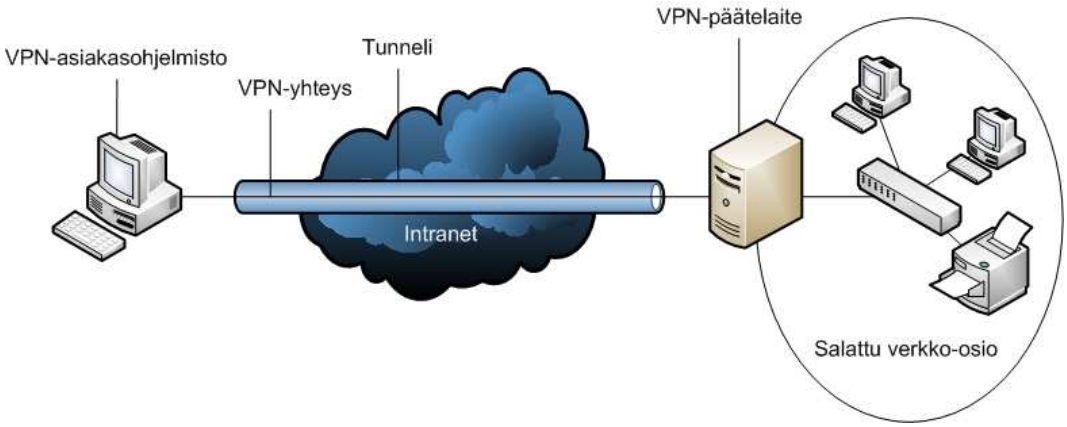
2.3 VPN-topologiat

VPN-topologiat voidaan jakaa karkeasti kahteen eri tyyppiin: yksittäinen etäyhteys ja Site-to-Site VPN, eli erilliset verkot yhdistävä VPN-yhteys. Yksittäinen etäyhteys mahdollistaa käyttäjälle, esimerkiksi kotona tai työmatkalla olevalle työntekijälle yhteyden tiettyyn yksityiseen verkkoon käyttäen julkisen verkon infrastruktuuria. Käyttäjälle VPN-yhteys näkyy point-to-point -linkkinä käyttäjän koneen (asiakasohjelmiston) sekä yrityksen verkossa olevan VPN-päätelaitteen välillä. Käyttäjän kone siis on loogisesti yrityksen sisäverkossa, kun käytetään VPN-yhteyttä, vaikka fyysisesti kone voi olla vaikka maapallon toisella puolella. Kuviossa 1 on kuvattu pelkistetysti yksittäinen VPN-yhteys. (Microsoft 2003b.)



KUVIO 1. Yksittäinen VPN-yhteys

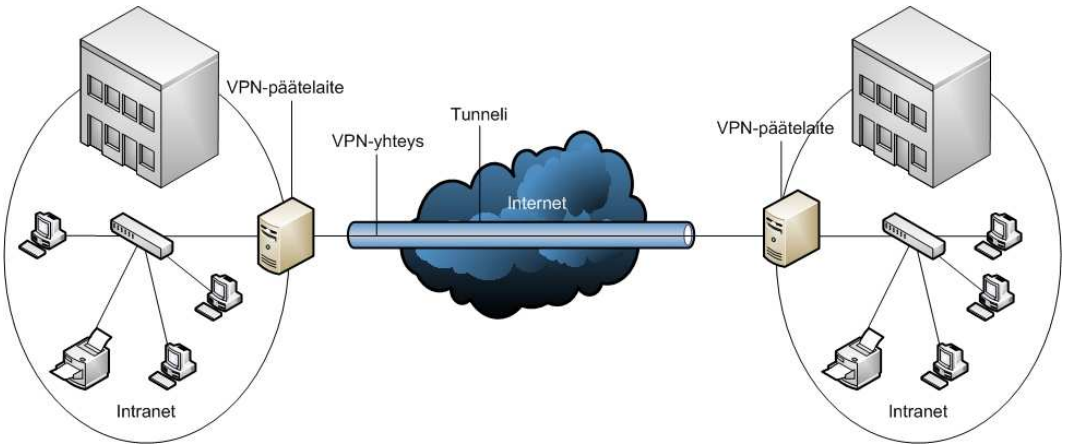
Yksittäistä VPN-yhteyttä voidaan käyttää myös yrityksen sisällä. Jokin osio sisäisestä verkosta voi olla kokonaan fyysisesti eristetty muusta verkosta, sillä kyseisen verkko-osion tiedot halutaan pitää erillään muusta sisäverkosta. Verkko-osio voi sisältää esimerkiksi hyvin luottamuksellisia, arkaluonteisia tietoja, joihin vain tietyillä työntekijöillä on saatavuus ja oikeus. Mutta koska verkko-osio on erillään muusta verkosta, täytyy edellä mainituilla työntekijöillä ola jonkinlainen mahdollisuus päästä siihen kiinni. VPN-yhteyden avulla voidaan kontrolloida työntekijöiden pääsyä verkko-osioon. Verkko-osioon sijoitetaan erillinen VPN-päätelaite, joka toimii vain VPN-käytössä, eikä siis reititä muuta liikennettä verkkojen välillä. Määritellyt työntekijät voivat avata VPN-yhteyden päätelaitteeseen ja saada näin suojatun verkko-osion resurssit ja tiedot käyttöönsä. Suojattu verkko-osio ei näy sellaisille käyttäjille, joilla ei ole siihen käyttöoikeuksia. Kuviossa 2 esitetään edellä mainittu VPN-ratkaisu. (Microsoft 2003a.)



KUVIO 2. Yksittäinen VPN-yhteys Intranetin yli

Site-to-Site VPN -yhteyttä käytetään, kun yhdistetään esimerkiksi eri tiloissa olevat sisäverkot. Molempien verkkojen käyttäjille toisessa päässä oleva verkko näkyy loogisesti ilman välissä oikeasti olevaa julkista verkkoa. Site-to-Site VPN-yhteyden muodostavat VPN-päätelaitteet, kuten palvelin, palomuuri tai reititin. VPN-päätelaitteet muodostavat tunnelin julkisen verkon yli. Kaikki verkkojen välinen liikenne reititetään salattuna tätä tunnelia pitkin, ja VPN-päätelaitteet huolehtivat saapuvan datan reitityksestä yksityiseen verkkoon. Liikenne salataan jonkin salausprotokollan sisään, eikä suojaus ole riippuvainen sovellustason protokollista. (Microsoft 2003b.)

VPN-päätelaitteet todentavat toisensa yhteyttä muodostettaessa. Yhteyden aloittava VPN-päätelaite (asiakas) todentaa ensin itsensä toiselle VPN-päätelaitteelle (palvelin), minkä jälkeen myös tämä VPN-päätelaite todentaa itsensä yhteyden avanneelle laitteelle. Kuviossa 3 esitetään pelkistetysti Site-to-Site VPN. (Microsoft 2003b.)



KUVIO 3. Site-to-Site VPN, kaksi verkkoa yhdistävä VPN-yhteys

3 VPN-TUNNELOINTIPROTOKOLLAT

3.1 IPsec

IPsec:iin viitataan usein protokollana, mutta todellisuudessa IPsec on protokollaperhe, jonka tarkoitus on suojata IP-pohjainen pakettiliikenne todentamalla ja salaamalla jokainen IP-paketti. IPsec:in määrittelemät protokollat voidaan jakaa kahteen eri luokkaan: pakettivirtojen turvaamiseen tarkoitetut protokollat ja turvattujen pakettivirtojen muodostamiseen tarkoitetut avaintenvaihtoprotokollat. Kaikki protokollat on määritelty RFC-dokumenteissa, joita valvoo IETF:n IPsec Working Group. (Wikipedia 2009a.)

IPsec toimii TCP/IP-mallin internettasolla, joka vastaa OSI-mallin kolmatta tasoa. Tämän takia se on joustavampi protokolla kuin ylemmillä tasoilla toimivat protokollat, kuten SSL, SSH ja TLS. IPsec:iä voidaan siis käyttää useampien liikennetyyppien salaamiseen, koska sovellusten ei tarvitse olla IPsec:iä varten suunniteltuja. (Wikipedia 2009a.)

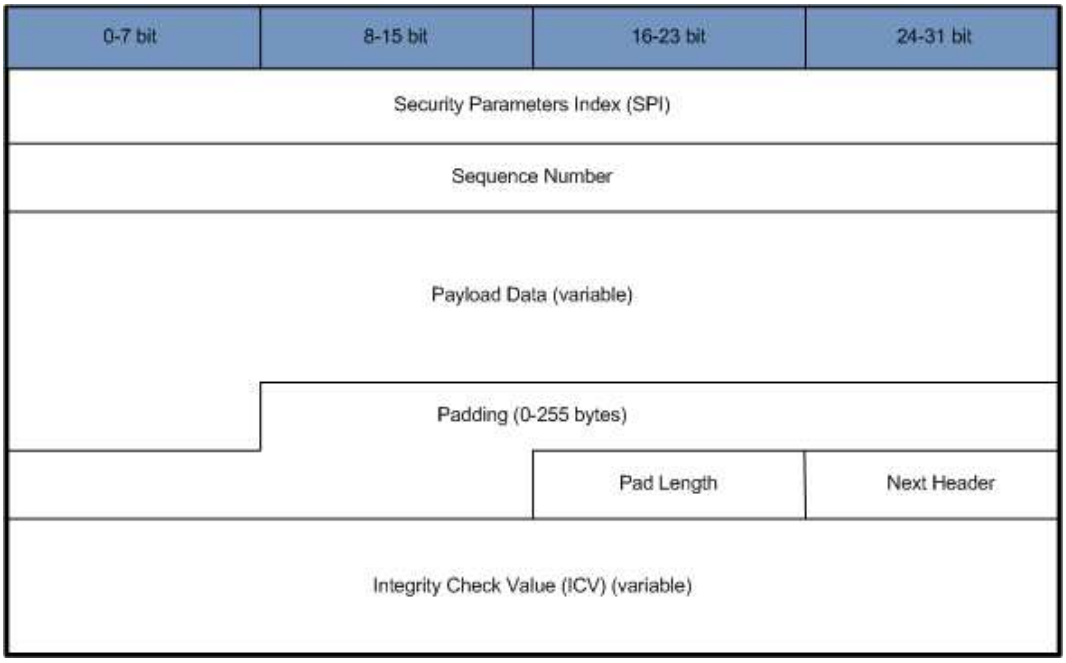
Seuraavissa kappaleissa käydään läpi IPsec:in pakettivirtojen turvaamiseen käyttämiä protokollia sekä avaintenvaihtoprotokollat. Lisäksi tutustutaan IPsec:in ja NATin yhteensopivuusongelmiin ja niiden ratkaisuihin.

3.1.1 Encapsulation Security Payload (ESP)

Encapsulation Security Payload on pakettivirtojen salaamiseen käytettävä protokolla. ESP tarjoaa datalle tietoturvan peruselementeistä luotettavuuden ja eheyden. Näiden lisäksi ESP voi taata datan alkuperän ja rajoitetusti myös pakettivirran luotettavuuden sekä hylätä toistetut paketit (anti-replay).
(Kent 2005.)

ESP voi toimia kahdessa eri toimintatilassa: Transport Mode ja Tunnel Mode. Transport-tilaa käytetään harvemmin sen rajoitetumman salauksen takia. Transport-tila soveltuukin lähinnä host-to-host -kommunikointiin. Tunnel-tilaa käytetään, kun halutaan yhdistää kokonaisia verkkoja VPN:n avulla sekä host-to-network -kommunikointiin. (Kent 2005.)

ESP toimii suoraan IP-protokollan päällä ja käyttää protokollanumeroa 50. Tämä arvo tulee löytyä ESP:n salaaman IP-paketin protokollaosiosta (IPv4) tai Next Header -osiosta (IPv6). Seuraavassa käydään ESP-paketti yksityiskohtaisemmin läpi. Kuviossa 4 on esitetty ESP-paketin rakenne. (Kent 2005.)



KUVIO 4. ESP-paketti

Security parameters index (SPI)

Pakollinen 32-bittinen arvo, jolla paketin vastaanottaja tunnistaa, mihin SA:han saapuva paketti on sidoksissa.

Sequence number

Pakollinen 32-bittinen kenttä, joka sisältää laskuriarvon. Laskuriarvo kasvaa yhdellä jokaisen lähetetyn paketin yhteydessä jokaisen SA:n sisällä. Sequence

number on siis 0 aina, kun uusi SA perustetaan. Sequence numberin avulla pystytään suojautumaan toistohyökkäyksiä vastaan.

Payload data

Muuttuvapituinen kenttä, joka sisältää siirrettävän datan.

Padding

0-255-bittinen kenttä, jolla täytetään data täysikokoiseksi blokiksi.

Pad length

Paddingin koko bitteinä.

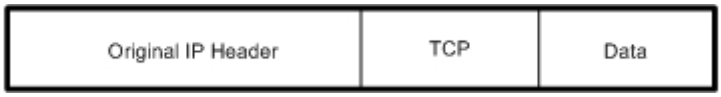
Next header

Pakollinen 8-bittinen kenttä, joka kertoo Payload data -kentän sisältämän datan tyypin. Next header -kentän arvo on siis jokin IP-protokollanumero.

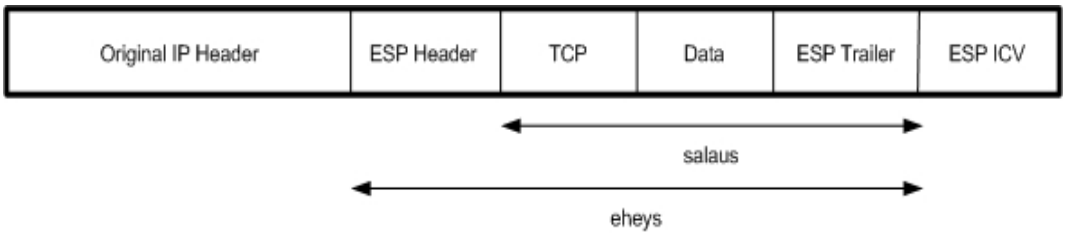
Integrity Check Value (ICV)

Muuttuvapituinen kenttä, joka lasketaan ESP-otsikon, Payload datan ja ESP trailer -kentän perusteella. ICV-kenttä sisältää datan, jolla autentikoidaan koko paketti.

Transport-tilassa ESP sijoitetaan alkuperäisen IP-otsikon ja Next Layer Protocol -kentän (esim. TCP, UDP, ICMP) väliin. Koska alkuperäistä IP-otsikkoa ei salata, ei paketin lähdeosoitteen eheyttä voida todentaa. Kuvioissa 5 ja 6 esitetään IPv4-paketti ennen ja jälkeen ESP:n lisäämisen. (Kent 2005.)

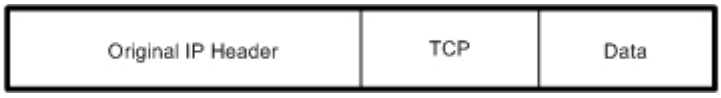


KUVIO 5. IPv4-paketti

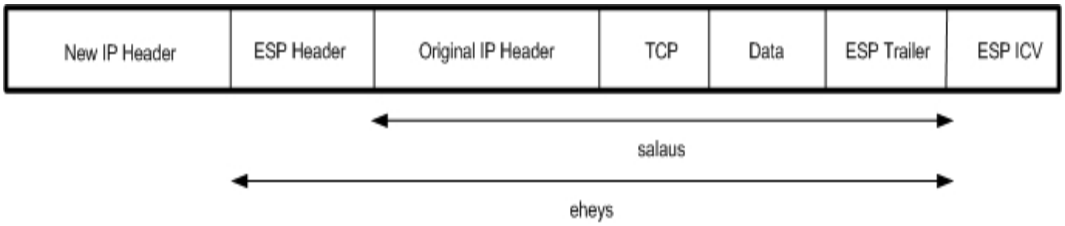


KUVIO 6. IPv4-paketti, ESP lisättynä, Transport-tila

Tunnel-tilassa IPv4-paketin alkuperäinen IP-otsikko jää ESP-kapsuloinnin sisään. ESP muodostaa uuden IP-otsikon, joka sisältää tunnelin muodostavan IPsec-laiteparin IP-osoitteet. Tunnel-tilassa ESP salaa koko alkuperäisen IP-paketin. Kuvioissa 7 ja 8 esitetään IPv4-paketti ennen ja jälkeen ESP:n lisäämisen. (Kent 2005.)



KUVIO 7. IPv4-paketti



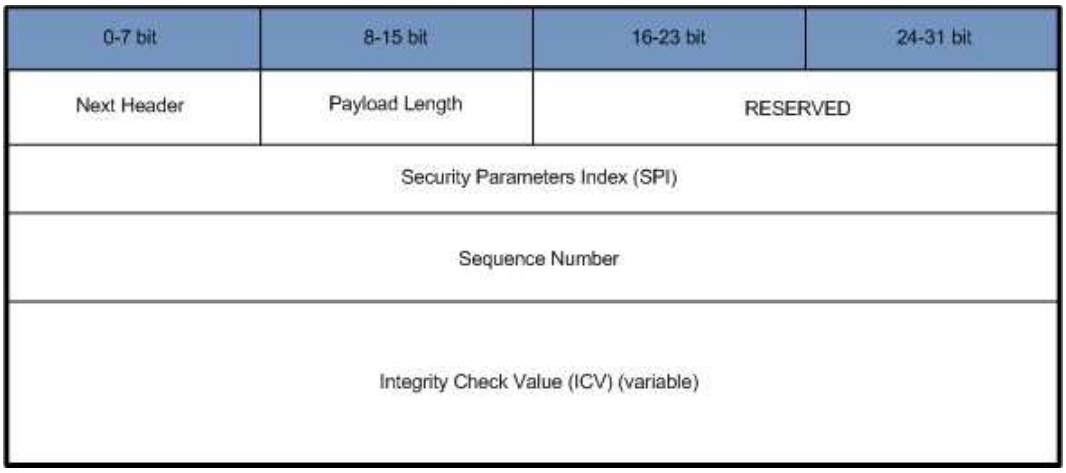
KUVIO 8. IPv4-paketti, ESP lisättynä, Tunnel-tila

3.1.2 Authentication Header (AH)

Authentication Header tarjoaa datalle eheyden ja alkuperän todennuksen mutta ei luottamuksellisuutta. AH tarjoaa myös suojan toistohyökkäyksiä vastaan, kuten ESP. AH suojaa siis aina sekä IP-paketin otsikon että datan (Kent & Atkinson 1998). IP-paketin otsikon suojaaminen aiheuttaa myös mahdollisesti ongelmia; mikäli IPsec-tunnelin muodostava laite on toisen reitittimen takana, tehdään sille todennäköisesti NAT, eli IP-paketin lähdeosoite muuttuu, ennen kuin paketti pääsee julkiseen verkkoon. Tämän johdosta AH:n suojaaman IP-paketin ICV, joka

on laskettu alkuperäisen IP-paketin kenttien perusteella, muuttuu, eikä vastaanottaja voi todentaa paketin alkuperää. (Aboba & Dixon 2004.)

AH toimii suoraan IP-protokollan päällä ja käyttää protokollanumeroa 51. Tämä arvo tulee löytyä AH:n salaaman IP-paketin protokollaosiosta (IPv4) tai Next Header -osiosta (IPv6). Seuraavassa käydään AH-paketti yksityiskohtaisemmin läpi. Kuviossa 9 on esitetty AH-paketin rakenne. (Kent & Atkinson 1998.)



KUVIO 9. AH-paketti

Next Header

8-bittinen kenttä, joka kertoo AH:ta seuraavan Payload –kentän sisältämän datan tyypin. Next header -kentän arvo on siis jokin IP-protokollanumero.

Payload Length

8-bittinen kenttä, joka määrittää AH:n pituuden 32-bittisinä sanoina, miinus 2. Jos esimerkiksi eheysalgoritmin todentamisarvo on 96-bittinen, olisi Payload Length -kentän arvo 4 (**3** 32-bittistä sanaa määrätyistä kentistä **+ 3** 32-bittistä sanaa ICV:stä **- 2**).

RESERVED

16-bittinen kenttä, joka on varattu tulevaa käyttöä varten. Siihen asti arvoksi tulee asettaa nolla.

Security Parameters Index (SPI)

Pakollinen 32-bittinen arvo jolla paketin vastaanottaja tunnistaa IP-osoitteiden lisäksi, mihin SA:han saapuva paketti on sidoksissa.

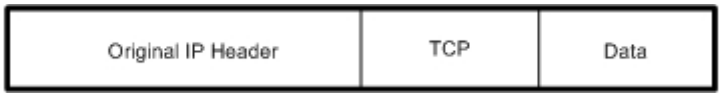
Sequence Number Field

Pakollinen 32-bittinen kenttä, joka sisältää laskuriarvon. Laskuriarvo kasvaa yhdellä jokaisen lähetetyn paketin yhteydessä jokaisen SA:n sisällä. Sequence number on siis 0 aina, kun uusi SA perustetaan. Sequence numberin avulla pystytään suojautumaan toistohyökkäyksiä vastaan.

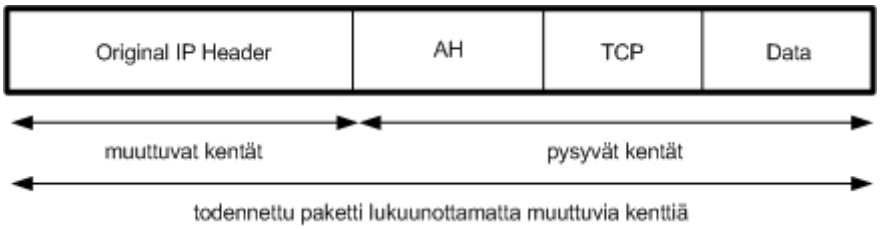
Integrity Check Value (ICV)

Muuttuvapituinen kenttä, joka sisältää paketin ICV-arvon. Kentän pituuden täytyy olla 32-bitillä jaollinen, joten se voi sisältää paddingia.

Kuten ESP, myös AH voi toimia sekä Transport- että Tunnel-tilassa. Transport-tilassa AH sijoitetaan alkuperäisen IP-otsikon ja Next Layer Protocol -kentän (esim. TCP, UDP, ICMP) väliin. Kuvioissa 10 ja 11 esitetään IPv4-paketti ennen ja jälkeen AH:n lisäämisen. (Kent & Atkinson 1998.)



KUVIO 10. IPv4-paketti

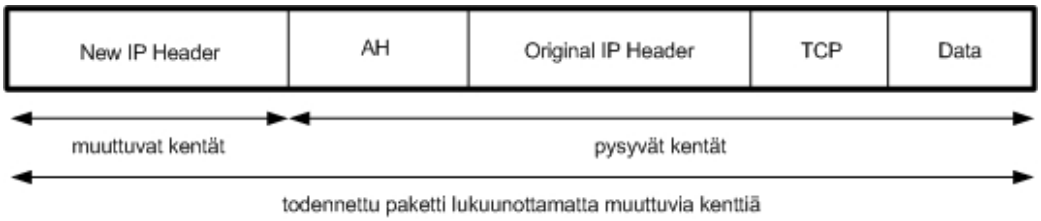


KUVIO 11. IPv4-paketti, AH lisättynä, Transport-tilassa

Tunnel-tilassa IPv4-paketin alkuperäinen IP-otsikko jää AH-kapsuloinnin sisään. AH muodostaa uuden IP-otsikon, joka sisältää tunnelin muodostavan IPsec-laiteparin IP-osoitteet. Tunnel-tilassa AH salaa koko alkuperäisen IP-paketin.

Kuvioissa 12 ja 13 esitetään IPv4-paketti ennen ja jälkeen AH:n lisäämisen. (Kent & Atkinson 1998.)

KUVIO 12. IPv4-paketti



KUVIO 13. IPv4-paketti, AH lisättynä, Tunnel-tilassa

3.1.3 Internet Key Exchange (IKE)

Internet Key Exchange on IPsec-protokollan kanssa käytettävä avaintenvaihtoprotokolla, jonka avulla IPsec muodostaa SA:n. IKE koostuu ISAKMP, Oakley ja SKEME -protokollien yhdistelmästä. (Carrel & Harkins 1998.)

ISAKMP tarjoaa kehykset todentamiselle ja avaintenvaihdolle, mutta ei määrittele niitä. ISAKMP määrittelee avaintenvaihdon vaiheet (phase). Oakley määrittelee erilaiset avaintenvaihdot eli tilat (mode) ja niiden tarjoamien palveluiden ominaisuudet. SKEME määrittelee mukautuvan avintenvaihtotekniikan. (Carrel & Harkins 1998.)

IKE käyttää Diffie-Hellman -avaintenvaihtoprotokollaa kahden autentikoidun osapuolen salausavaimen sopimiseen (Carrel & Harkins 1998). Autentikointiin käytetään yleensä joko etukäteen sovittua, manuaalista salattua avainta (Pre-shared key, PSK) tai X.509-sertifikaatteja. Esijaettu avain eli PSK on yksinkertainen määritellä ja hyvä ratkaisu VPN-tunnelin testauksessa ja ongelmanratkaisussa. PSK täytyy valita huolellisesti, jotta edes jonkinlainen tietoturva voidaan taata.

PSK on altis brute force -hyökkäyksille, ja lisäksi PSK:n skaalautuvuus on ongelmallinen laajemmissa kokonaisuuksissa, sillä avain täytyy asettaa manuaalisesti jokaiseen laitteeseen. X.509 -sertifikaatit perustuvat julkisen avaimen kryptografiaan (Public-key cryptography). (Housley, Ford, Polk & Solo, 1999.)

IPsec VPN -tunneli muodostetaan yleensä kahdessa vaiheessa, joista kumpikin määrittelee SA:n, joka puolestaan määrittelee tunnelin muodostavien osapuolien salauksessa käytettävät parametrit ja arvot. Ensimmäisessä vaiheessa (Phase 1) kaksi ISAKMP-osapuolta muodostavat turvatun ja todennetun siirtotien, jota kutsutaan IKE Security Association-nimellä. Ensimmäisen vaiheen päättää jompikumpi Oakleyn määrittelemistä tiloista: Main mode tai Aggressive Mode. Toisessa vaiheessa (Phase 2) kaksi osapuolta muodostavat IPsec SA:n, jonka läpi osapuolet voivat lähettää ja vastaanottaa dataa. (Carrel & Harkins 1998.)

3.1.4 Salausalgoritmit

IKE ja IPsec käyttävät pakettien salaamiseen erinäisiä salausalgoritmeja. Salausalgoritmit voivat olla kryptografisia tiivistefunktioita, kuten MD5 ja SHA-1 tai symmetrisiä lohkosalausmenetelmiä, kuten DES, 3DES ja AES. Tiivistefunktiot perustuvat kahteen pääajatukseen: algoritmin tuottamasta tiivisteestä ei tule voida päätellä salatusta tiedosta mitään ja algoritmin tuottamien tiivisteiden tulee jakautua arvaamattomasti (Viestintävirasto 2007b). Lohkosalausmenetelmät puolestaan salaavat nimensä mukaisesti yhden lohkon tietoa kerrallaan (Viestintävirasto 2007a).

MD5-algoritmilla tuotetaan 128-bittinen tiiviste, joka yleensä esitetään 32-merkkisenä heksakoodatussa muodossa. SHA-1 on MD5-algoritmin seuraaja, ja se on julkaistu Yhdysvaltojen hallituksen standardina. SHA-1-algoritmi tuottaa 160-bittisen tiivisteen samankaltaisin keinoin kuin MD5. Kuten MD5, myös SHA-1 on jo onnistuttu murtamaan. Siitä onkin kehitetty turvallisempia versioita, jotka ovat SHA-2 ja kehitteillä oleva SHA-3. (Wikipedia 2009e.)

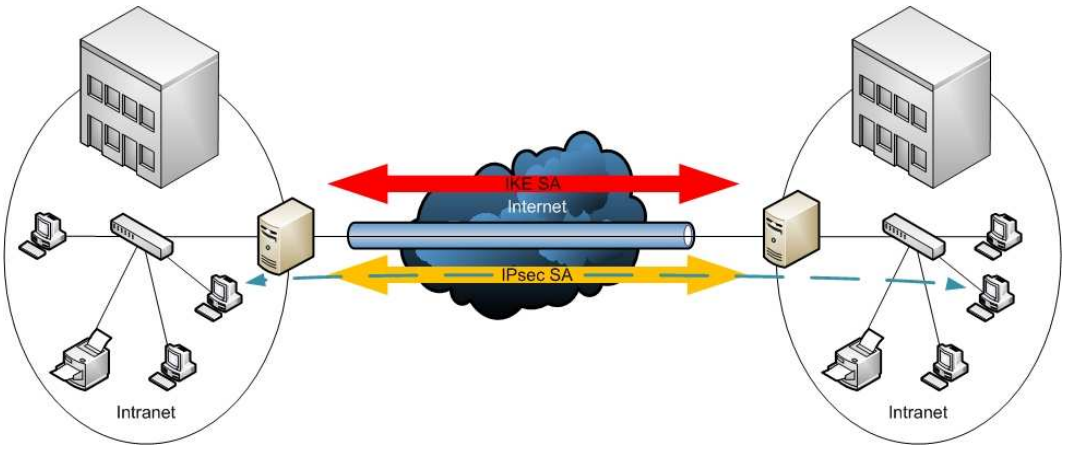
DES, 3DES, AES ovat symmetrisiä lohkosalausmenetelmiä. DES salaa 64-bittisiä lohkoja 56-bittisellä avaimella. Nykyisillä tehokkailla koneilla DES on nopea murtaa käyttämällä brute force -menetelmää, joten sen käyttöä ei enää nykyään suositella VPN:n yhteydessä. 3DES on DES-salauksen muoto, joka käyttää samaa algoritmia kuin DES, mutta lisää suojauskertoja. Jokainen suojattava lohko siis salataan kolme kertaa käyttämällä DES-algoritmia. AES on nykyisin käytettäväksi suositeltu lohkosalausmenetelmä. AES salaa 128-bittisiä lohkoja 128, 192 tai 256-bittisellä avaimella. Toitaiseksi AES on murtamaton, ja sitä käytetäänkin mm. Yhdysvaltojen hallituksen asiakirjojen salaamiseen. (Salausmenetelmät 2008.)

3.1.5 Security Association (SA)

Security Association tarkoittaa IPsec-tunnelin muodostavien laitteiden välistä suhdetta ja määrittelee, kuinka osapuolet käyttävät turvallisuusasetuksia kommunikointiin. SA:n avulla IPsec siis pitää kirjaa tiettyyn IPsec-istuntoon liittyvistä yksityiskohdista. SA:n konsepti on keskeinen IPsec:in kannalta. (Mason 2002.)

IPsec antaa monia keinoja salaukseen ja todentamiseen. Jokainen IPsec-yhteys voi tarjota salauksen, eheyden ja todentamisen. Kun IPsec-yhteys perustetaan, täytyy osapuolten määritellä, mitä salausalgoritmeja käytetään ja jakaa istunnon avaimet. IPsec-yhteys käyttää kahta eri SA:ta: IKE SA ja IPsec SA. IKE SA määrittelee osapuolten salausasetukset ja -parametrit. IPsec SA määrittelee verkkotiedot, aktiiviset protokollat (AH/ESP) ja kapsuloinnin. Jokainen SA siis sisältää arvoja, kuten SPI:n, kohdeosoitteen, salaustavat ja -avaimet ja IPsec:in elinaika (lifetime). (Mason 2002.)

VPN-yhteys muodostetaan kahdessa vaiheessa, joista molemmissa perustetaan SA. Ensimmäisessä vaiheessa perustetaan IKE SA, jonka jälkeen IPsec SA voidaan perustaa turvallisesti toisessa vaiheessa. Kuviossa 14 on kuvattu edellä mainitut SA:t. (Mason 2002.)



KUVIO 14. IKE SA ja IPsec SA

SA on yksisuuntainen, eli päätelaiteparilla on vähintään kaksi tietoturvayhteyttä; yhteyden avaaja eli asiakas lähettää vastaanottajalle eli palvelimelle SA:n – jos vastaanottaja hyväksyy tämän, lähettää se SA:n takaisin yhteyden avaajalle. Tämä prosessi muodostaa kaksi yksisuuntaista SA:ta osapuolten välille. Kaksisuuntainen liikenne koostuu siis kahdesta SA:sta, yksi kumpaankin suuntaan. (Mason 2002.)

3.1.6 NAT-T

NAT Traversal on IPsec:in suojaamien IP-pakettien NAT-laitteiden läpäisyyn avustava tapa. NAT-T on kehitetty vastaamaan IPSec:in ja NAT:in yhteensopivuusongelmiin. NAT eli osoitteenmuunnos on hyvinkin yleinen monissa kohteissa, kuten kodeissa ja hotelleissa, ja koska etäyhteyksiä käytetään ensisijaisesti edellämainituissa kohteissa, täytyi ongelmaan saada ratkaisu jo käytettävyyden kannalta (Wikipedia 2009c). Seuraavassa IPsec:in ja NAT:in yhteensopivuusongelmia:

IPsec AH ja NAT

AH käyttää IP-paketin otsikkoa, joka sisältää paketin lähde- ja kohdeosoitteen, ICV:n laskemiseen eli paketin todentamiseen. NAT puolestaan suorittaa osoitteenmuunnoksen paketille, eli muuttaa lähdeosoitteen, jolloin ICV:stä tulee

virheellinen ja paketin vastaanottaja hylkää paketin. ESP:tä käytettäessä tätä ongelmaa ei tule, koska ESP ei käytä lähde- ja kohdeosoitetta ICV:n laskemiseen. (Aboba & Dixon 2004.)

Tarkistussummat ja NAT

TCP- ja UDP-otsikot sisältävät tarkistussumman, jonka laskemiseen on käytetty paketin lähde- ja kohdeosoitetta sekä porttinumeroita. Normaalisti NAT päivittää tarkistussumman muuttaessaan IP-osoitetta tai porttinumeroa, mutta ESP:n salaamaan pakettiin NAT ei voi päivitystä tehdä. Tämän takia tarkistusumma on virheellinen, kun paketti saapuu vastaanottajalle. (Aboba & Dixon 2004.)

IKE-osoitetunnisteet (address identification) ja NAT

IKE-protokolla voi käyttää IP-osoitteita IPsec-osapuolten tunnistamiseen tunnelin muodostamisen vaiheissa 1 (Main/Aggressive) ja 2 (Quick). Koska NAT vaihtaa IP-paketin lähdeosoitteen, vastaanottajalle saapuessaan IKE:n tunnisteessa käyttämä alkuperäinen lähdeosoite ei enää vastaa paketin nykyistä lähdeosoitetta. Tämän johdosta vastaanottaja, eli toinen IPsec-osapuoli, hylkää paketin. Ongelma voidaan kiertää käyttämällä IKE:n tunnisteena esimerkiksi userID:tä tai FQDN:tä IP-osoitteiden sijaan. (Aboba & Dixon 2004.)

IKE:n UDP-porttinumero

IKE käyttää UDP-porttia 500 sekä lähde- että kohdeporttina. Mikäli NAT tekee IP-paketille osoitteenmuunnoksen lisäksi myös porttimuunnoksen (NAPT), ei paketin vastaanottaja, eli toinen IPsec-osapuoli, ymmärrä, että kyseessä on IPsec-liikenne ja mahdollisesti hylkää paketin. Tämä pätee erityisesti ensimmäisen (initial) IKE-paketin suhteen. (Aboba & Dixon 2004.)

Sulautetut (embedded) IP-osoitteet ja NAT

IPsec salaa IP-paketit, joten paketin sisälle jäävät IP-osoitteet eivät ole NAT:in muunneltavissa. Tämä vaikuttaa NAT:illa toteutetun Application Layer Gatewayn toimintaan. ALG on NATin toteutus jollekin tietylle sovellusprotokollalle, kuten FTP, H.323 tai SIP. ALG suorittaa protokollaan vaatimat muutokset paketin rakenteeseen. Ongelma on ratkaistavissa asentamalla ALG itse IPsec-osapuoleen,

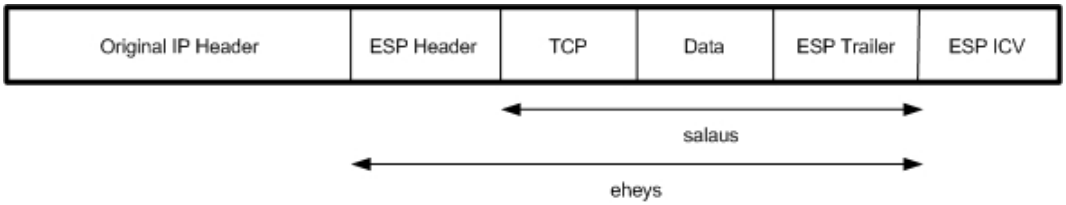
eli työasemaan tai VPN-laitteeseen, jotta ALG voi toimia ennen IPsec-kapsulointia ja kapsuloinnin poiston jälkeen. (Aboba & Dixon 2004.)

IPsec-liikenteen kanavointi

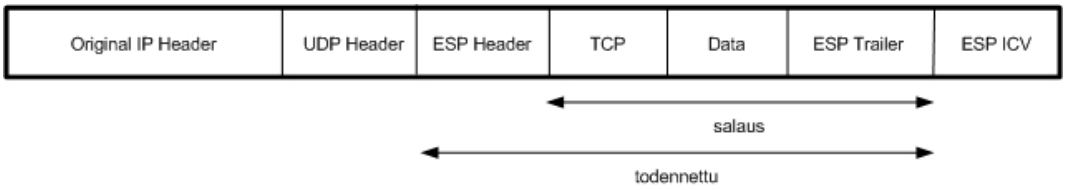
ESP-kapsuloiduissa IP-paketeissa ei ole näkyvää TCP- tai UDP-otsikkoa, koska ESP salaa kyseiset kentät. Tämän takia TCP- ja UDP-porttinumeroita ei voida käyttää kanavoimaan liikennettä useille eri isännille yksityisessä verkossa NAT-laitteen takana. NATin täytyy mapata paketin kohdeosoite yksityiseen osoitteeseen, jotta se voi vastaanottaa sisäänpäin tulevaa liikennettä. Kun NAT vastaanottaa useita IPsec-datavirtoja, jotka on kapsuloita ESP:llä, on kaikkien pakettien kohdeosoite sama. Ongelman ratkaistakseen NAT mappaa kohdeosoitteen IPsec-paketin SPI-arvoon. Nyt NAT pystyy erottamaan jokaisen vastaanotetun IP-sec-paketin ja lähettämään sen oikealle isännälle. (Aboba & Dixon 2004.)

IPsec NAT-T lisää IP-pakettiin UDP-otsikon, joka kapsuloi ESP-otsikon. Tällä toiminnolla NAT-reitittimille annetaan mahdollisuus kanavoida IPsec-liikennettä, koska NAT saa näkyvän UDP-otsikon ja sen myötä UDP-portin. Lisäksi NAT-T laittaa alkuperäisen IP-osoitteen NAT-OA (Original Address) kenttään. Tämän avulla IPsec-osapuolet näkevät myös alkuperäiset IP-osoitteet ja portit ja voivat todentaa tarkistussummat. Kuvioissa 15, 16, 17 ja 18 on esitetty UDP-kapselointi Tunnel- ja Transport-tiloissa. (Huttunen, Swander, Volpe, DiBurro & Stenberg 2005)

NAT-T, ESP Transport-tilassa



KUVIO 15. IPv4-paketti, ESP lisättynä, Transport-tila



KUVIO 16. IPv4-paketti, ESP ja UDP lisättynä, Transport-tila

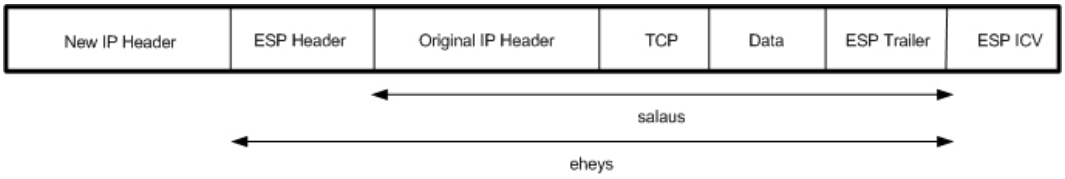
Kapsulointi:

1. IP-paketti on kapsuloitu ESP:n sisään.
2. UDP-otsikko lisätään.
3. IP-otsikon Total Length, Protocol ja Header Checksum -kenttien arvot päivitetään uutta IP-pakettia vastaaviksi.

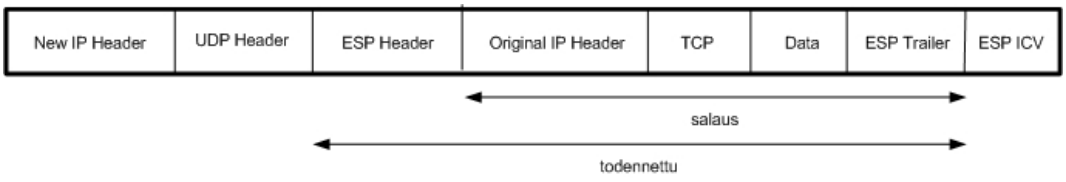
Kapsuloinnin poistaminen:

1. UDP-otsikko poistetaan.
2. IP-otsikon Total Length, Protocol ja Header Checksum -kenttien arvot päivitetään IP-pakettia vastaaviksi.
3. ESP-kapsulointi poistetaan.
4. Transport-tilan kapsulointi poistetaan NAT-toiminnolla.

NAT-T, ESP Tunnel-tilassa



KUVIO 17. IPv4-paketti, ESP lisättynä, Tunnel-tila



KUVIO 18. IPv4-paketti, ESP ja UDP lisättynä, Tunnel-tila

Kapsulointi:

1. IP-paketti on kapsuloitu ESP:n sisään.
2. UDP-otsikko lisätään.
3. IP-otsikon Total Length, Protocol ja Header Checksum -kenttien arvot päivitetään uutta IP-pakettia vastaaviksi.

Kapsuloinnin poistaminen:

1. UDP-otsikko poistetaan.
2. IP-otsikon Total Length, Protocol ja Header Checksum -kenttien arvot päivitetään IP-pakettia vastaaviksi.
3. ESP-kapsulointi poistetaan.
4. Tunnel-tilan kapsulointi poistetaan NAT-toiminnolla.

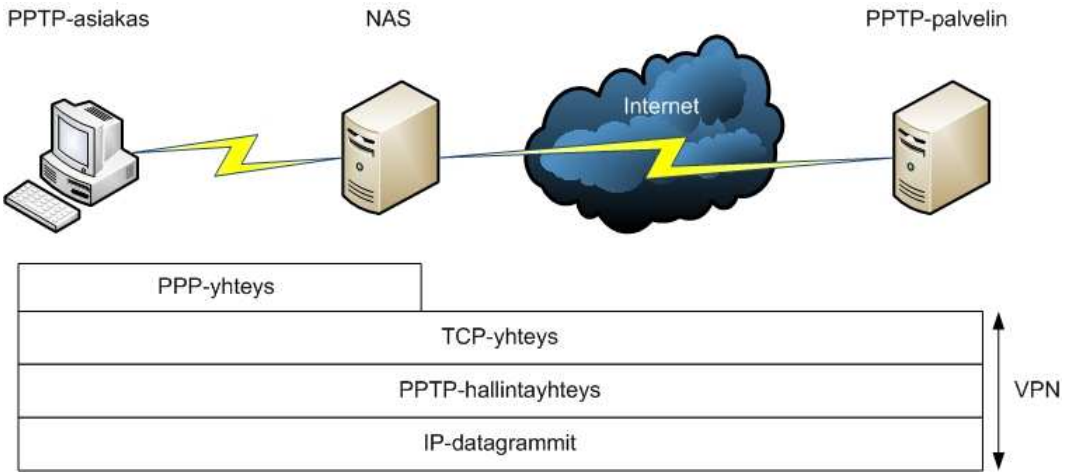
3.2 PPTP

Point-to-Point -tunnelointiprotokolla on PPP-protokollan laajennus, joka mahdollistaa turvallisen tiedonsiirron kahden osapuolen välille luomalla VPN-tunnelin TCP/IP-pohjaisen verkon päälle. PPTP on Microsoftin, Ascend Communicationsin (nykyään osa Alcatel-Lucentia) ja 3COMin kehittämä protokolla. Alunperin PPTP oli tarkoitettu Windows-työasemien liittämiseen Windows-palvelimille julkisen verkon yli. Microsoftin mukanaolon johdosta PPTP onkin laajalle levinnyt ja vielä edelleen hyvin yleisesti käytössä oleva tunnelointiprotokolla. PPTP on toteutettuna Windows-käyttöjärjestelmissä, jolloin esimerkiksi erillisiä asiakasohjelmistoja ei tarvita, kuten IPsec:in kanssa. (Wikipedia 2009b.)

PPTP käyttää liikennöintiin hallintapaketteja ja datapaketteja. Hallintapaketteja PPTP käyttää tilantiedusteluun ja merkinantoon. Hallintapaketit kulkevat PPTP-tunnelin päätepisteiden välille luodun TCP-yhteyden välityksellä. Datapaketit sisältävät varsinaisen käyttäjädatan. PPTP käyttää GRE-protokollaa pakettien tunneloimiseen ja välittämiseen. (Hamzeh, Pall, Verthein, Taarud, Little & Zorn 1999.)

PPTP:n toteuttamiseen liittyy kolme laitetta: PPTP-asiakas, Network Acccess Server (NAS) ja PPTP-palvelin. NAS voidaan jättää pois, jos PPTP-tunnelin muodostetaan samassa lähiverkossa olevien laitteiden välille. Yleisimmät PPTP:n toteuttamismallit ovat asiakas-palvelin, RAS-palvelin ja palvelin-palvelin. Seuraavassa kappaleessa kuvataan tyypillinen PPTP-skenaario. (Microsoft 2009.)

PPTP-asiakas ottaa PPP-yhteyden palveluntarjoajan NAS:iin. Yhteyden muodostettuaan asiakas voi lähettää ja vastaanottaa paketteja julkisen verkon yli. Seuraavaksi asiakas luo muodostetun PPP-yhteyden läpi toisen yhteyden, TCP-yhteyden, jota pitkin datapaketit lähetetään. Lähetetyt datapaketit ovat IP-datagrammeja, jotka sisältävät GRE-kapsuloituja PPP-paketteja. Edellä mainittu TCP-yhteys luo VPN-tunnelin kohteena olevaan PPTP-palvelimeen. Prosessi on kuvattu kuviossa 19. (Microsoft 2009.)



KUVIO 19. PPTP-yhteys

PPTP:ssä on monia turvallisuusongelmia, kuten todentamattomat TCP-paketit ja hallintapaketit sekä heikko todennus, johon käytetään vain CHAP-protokollaa. PPTP-protokollan kehittäminen onkin melkolailla pysähtynyt, ja korvaaviksi tunnelointiprotokolliksi on nousemassa L2TP sekä IPsec. Päivittäminen on kuitenkin ollut hidasta PPTP:n helppokäyttöisyyden vuoksi, kun sitä verrataan monimutkaisempiin tunnelointiprotokolliin. (Wikipedia 2009d.)

3.3 L2TP

L2TP on verkkoprotokolla, joka kapseloi turvattomien verkkojen yli lähetettävät PPP-paketit. Verkot voivat olla IP-, Frame Relay- tai ATM-verkkoja. L2TP yhdistää Ciscon Layer 2 Forwarding (L2F) -protokollan ja PPTP:n parhaat puolet. (Cisco Systems, Inc. 2006.)

Kuten PPTP, L2TP käyttää liikennöintiin hallintapaketteja ja datapaketteja. Hallintapaketeilla perustetaan ja ylläpidetään tunneleita sekä suljetaan tunnelit yhteyden päätteeksi. Hallintapaketeissa L2TP käyttää UDP:tä ja L2TP-pohjaisia viestejä. Datapaketteihin kapseloidaan tunneliin lähetettävät PPP-paketit. L2TP tarjoaa luotettavan tiedonsiirron hallintapaketeille, mutta ei datapaketeille. Datapakettien luotettavaan tiedonsiirtoon L2TP-tunnelissa käytetään muita protokollia. (Wikipedia 2009b.)

L2TP-tunneli luodaan kutakuinkin samalla tavalla kuin PPTP-tunneli. L2TP-tunnelin luovia osapuolia kutsutaan nimillä L2TP Access Concentrator (LAC) ja L2TP Network Server (LNS). LAC on L2TP-tunnelin luoja ja LNS tunnelipyynnöt vastaanottava osapuoli. L2TP-tunnelia luotaessa tunnistautuminen tapahtuu, kuten PPP:ssä. L2TP käyttää PPP:n pakkausmenetelmää, mutta ei sen salausmenetelmää. Salaukseen L2TP käyttää yleensä IPsec:iä, jolla voidaan taata luottamuksellisuus, todentaminen ja eheys L2TP-paketeille. Kun L2TP-tunneli on luotu, on siinä kulkeva liikenne kaksisuuntaista. (Wikipedia 2009b.)

3.4 SSL VPN

SSL VPN (Secure Sockets Layer VPN) -tekniikka mahdollistaa VPN-yhteyksien käytön käytännössä millä tahansa internetselaimella. SSL VPN:n alkuperäinen tarkoitus olikin ratkaista monimutkaisten ja vaikeasti toteutettavien VPN-ratkaisuiden tuottamia ongelmia. SSL VPN ei vaadi käyttäjän koneelle esiasennettavia asiakasohjelmistoja, kuten esimerkiksi IPsec. Perinteisesti SSL VPN -yhteyksillä käytetään selainpohjaisia sovelluksia tai sähköpostia, mutta

uudemmat SSL VPN -tekniikat mahdollistavat myös verkkokerroksella toimivien sovellusten käytön. SSL VPN toteutetaan VPN-laitteiden avulla; käyttäjä ottaa selaimella yhteyden SSL VPN -laitteeseen, joka muodostaa SSL-tunnelin työaseman ja SSL VPN -laitteen välille. (Techtarget 2009.)

SSL VPN -tekniikka tarjoaa monipuolisen ja helppokäyttöisen VPN-ratkaisun. SSL VPN mahdollistaa käyttäjille pääsyn haluttuihin resursseihin sijainnista riippumatta. SSL VPN voidaan jakaa kahteen pääryhmään: portaali ja tunneli. SSL VPN -portaalissa käyttäjä muodostaa selaimella SSL yhteyden SSL VPN -laitteeseen. Käyttäjä tunnistautuu laitteen määrittelemällä tavalla, minkä jälkeen selaimeen avautuu internetsivu, jota kutsutaan portaaliksi. Tältä sivulta päästään käyttämään määriteltyjä palveluja ja resursseja. SSL VPN -portaali on yleisimmin käytetty SSL VPN -tekniikka. SSL VPN -tunneli laajentaa SSL VPN:n toimivuuden verkkokerrokselle. SSL VPN -tunnelilla käyttäjän on mahdollista käyttää sovelluksia ja protokollia, jotka eivät ole selainpohjaisia. Liikenne kulkee tällöin SSL-tunnelia pitkin. SSL VPN -tunnelia käytettäessä selaimen on tuettava aktiivista sisältöä (active content), kuten Javaa, Active X:ää tai Flashiä. (Techtarget 2009.)

3.5 Tunnelointiprotokollien vertailu

IPsec ja SSL VPN ovat yleisimmin käytettyjä tunnelointiprotokollia. Valinta näiden protokollien välillä tehdään yleensä käyttötarkoituksen mukaan. Mikäli etäyhteyksillä käytettävät sovellukset ja resurssit ovat toteutettavissa SSL VPN:n avulla, on se yleensä suositellumpi vaihtoehto huomattavasti helpomman käyttöönoton ja konfiguroinnin takia. IPsec-protokollaa käytetään, kun halutaan muodostaa etäyhteys kokonaiseen verkkoon tai yhdistää verkkoja toisiinsä julkisen tiedonsiirtokanavan läpi.

IPsec-tunnelointiprotokollaa käytettäessä tulee ottaa huomioon myös laitevalmistajien väliset yhteensopivuusongelmat. Yleensä suositellaankin käytettävän saman valmistajan laitteita muodostettaessa IPsec-tunneleita. IPsec on

toisaalta standardoitu protokolla, mitä SSL VPN ei ole. Perinteinen SSL VPN toimii OSI-tasoilla 4-7, joten verkkokerroksen sovellusten käyttö ei ole sillä mahdollista. SSL VPN -tunnelit kuitenkin laajentavat toiminnan myös OSI-tasolle 3, eli verkkokerrokselle, jolloin SSL VPN vastaa IPsec-tunnelia käyttösoveltuvuuden suhteen.

Tunnelointiprotokollista PPTP ja L2TP ovat hyvin samankaltaisia. Molempien pohjana ovat PPP-paketit, joihin lisätään tunneloinnin vaatimat otsikkotiedot. Protokollien välillä on kuitenkin muutamia eroavaisuuksia:

- PPTP salaa siirrettävän datan vasta PPP-yhteyden luontiprosessin jälkeen, L2TP- yhteys on salattu jo ennen PPP-yhteyden muodostamista
- PPTP-yhteyksissä käytetään vain käyttäjäkohtaista autentikointia, L2TP-yhteydet käyttävät lisäksi konekohtaista autentikointia sertifikaattien avulla

Käyttötarkoituksesta riippuen molemmilla protokollilla on siis omat vahvuutensa toiseen verrattuna. L2TP-yhteydet tarjoavat vahvemman autentikoinnin käyttämällä sekä käyttäjäkohtaista että konekohtaista sertifikaattipohjaista autentikointia. PPTP-yhteydet ovat puolestaan helpompia toteuttaa, koska sertifikaattien käsittelyä ei vaadita. Lisäksi PPTP on laajemmin tuettu tunnelointiprotokolla.

4 ETÄYHTEYSRATKAISUN SUUNNITTELU JA TOTEUTTAMINEN

4.1 Yrityksen esittely

Opinnäytetyö tehtiin hankkeistettuna projektina Lahti Precision Oy:lle. Lahti Precision Oy on punnitus- ja annostusjärjestelmien ja laitosten, vaakojen, punnituskomponenttien ja punnitusalan kunnossapitopalveluiden toimittaja. Lahti Precision Oy:n ensisijaisia asiakkaita ovat lasiteollisuus sekä laasti- ja tasoiteteollisuus. Lasitehtaiden raaka-ainelaitosten ja laastitehtaiden toimittajana Lahti Precision Oy on yksi maailman suurimmista, ja punnitusalalla Lahti Precision Oy on Suomen suurin yritys. Lahti Precision Oy:n toimipisteet sijaitsevat Lahdessa Sopenkorvessa, Paraisilla, Jyväskylässä ja Shanghaissa Kiinassa. Opinnäytetyöprojekti toteutettiin Lahden toimipisteessä.

4.2 Etäyhteyksien alkutilanne

Lahti Precision Oy käyttää etäyhteyksiä asiakastehtaiden prosessiverkkojen monitorointiin ja vikatilanteissa ongelmanratkaisuun. Etäyhteyksien avulla poistetaan asiantuntijainsinöörien matkustustarve ja vasteaika vikatilanteissa pienenee. Etäyhteyksillä päästään kiinni prosessiverkoissa oleviin ohjelmoitaviin logiikoihin, vaakaohjaimiin ja palvelinkoneisiin.

Alunperin opinnäytetyöprojektin tavoitteena oli tuotteistaa tietoliikenneyritykseltä ostettuna palveluna hankittuja etäyhteyksiä. Tuotteistamalla Lahti Precision Oy:n olisi helpompi myydä ja toteuttaa etäyhteysratkaisuja. Tietoliikenneyritykseltä ostetusta etäyhteyspalvelusta olisi täytynyt tehdä kolmen vuoden kiinteähintainen sopimus, joka ei Lahti Precision Oy:n kannalta ollut mielekästä. Jokaiselle asiakastehtaalle olisi täytynyt tehdä erillinen sopimus, jolloin etäyhteyspalvelun kustannukset olisivat karanneet liian korkeiksi. Etäyhteyksien käyttö on satunnaista, eikä sopimuksen hinnasto korreloinut etäyhteyksien käyttötarpeeseen.

Lahti Precision Oy:llä ei liity etäyhteyksiin suoranaista liiketoimintaa, vaan ne tarjotaan asiakastehtaisiin takuuajaksi, minkä jälkeen jatkosta sovitaan erikseen.

Hyvin aikaisessa vaiheessa opinnäytetyöprojektia päätettiinkin, että etäyhteysratkaisuja ei hankita ostettuna palveluna vaan ne toteutetaan itse. Tällöin Lahti Precision Oy:llä on suurempi kontrolli etäyhteyksien toteustusratkaisuihin ja kuluihin. Lisäksi poistetaan yksi välikäsi etäyhteyspalvelusta, kun palvelu toteutetaan vain Lahti Precision Oy:n ja asiakasyrityksen kesken.

Aiemmat etäyhteysratkaisut yrityksessä olivat suurilta osin puhelinmodeemipohjaisia. Puhelinmodeemit eivät aiheuta kiinteitä kuluja ja niiden toimintavarmuus on ollut kiitettävää. Puhelinmodeemeilla toteutetut etäyhteydet eivät kuitenkaan enää nykyaikaisessa tiedonsiirrossa ole mielekäs vaihtoehto. Kansainväliset puheluhinnastot tulevat hyvin kalliiksi, eivätkä tiedonsiirtonopeudet eivät ole samalla tasolla vaatimusten kanssa. Lisäksi puhelinmodeemipohjaisilla ratkaisuilla saadaan usein yhteys vain yhteen laitteeseen, kun mielekkäämpää on saada etäyhteys kokonaiseen verkkoon.

Yrityksen asiakkaat tarjosivat myös omia etäyhteysratkaisujaan, jotka perustuivat yleensä VPN-asiakasohjelmistoihin. Asiakkaalla on siis oma VPN-päätelaite, johon VPN-asiakasohjelmistolla otetaan yhteys Lahti Precision Oy:ltä ja luodaan näin VPN-tunneli. VPN-asiakasohjelmistojen kanssa ongelmaksi muodostuu niiden yhteensopivuus. Kun samalle työasemalle asennettiin useita eri VPN-asiakasohjelmistoja, muodostui toimivuusongelmia yhteyksien kanssa, jolloin ratkaisuksi jäi pitää vain yhtä VPN-asiakasohjelmistoa asennettuna. Eri asiakkailla on eri valmistajien VPN-asiakasohjelmistoja, joten käytännössä jokaiselle asiakkaalle piti olla oma työasema, jolta VPN-yhteys avattiin.

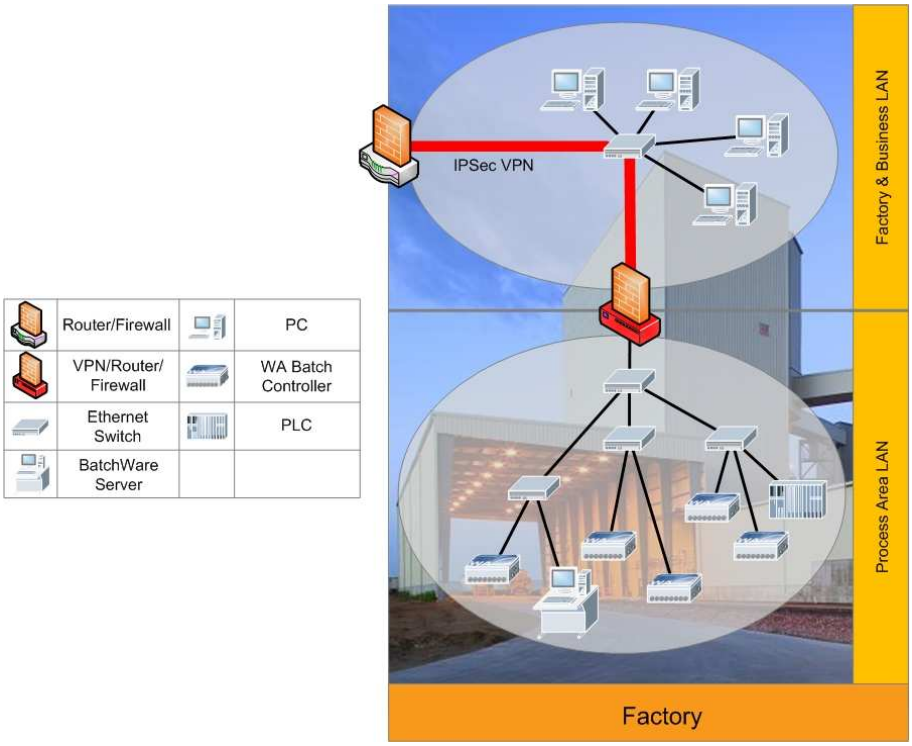
Projektin tavoitteena olikin luoda Lahti Precision Oy:lle toimiva ja skaalautuva etäyhteysratkaisu. Etäyhteysratkaisun tulisi perustua standardeihin ja olla laitteistopohjainen, jotta VPN-asiakasohjelmistojen käyttöä ei tarvita. Etäyhteysratkaisu tulisi käyttämään laajakaistayhteyksiä vastatakseen tiedonsiirtonopeuden tarpeeseen. Tuotteistamalla suunniteltu etäyhteysratkaisu,

voidaan sitä helpommin tarjota ja myydä uusille asiakkaille ja etäyhteysratkaisun toteuttaminen on helpompaa.

4.3 Etäyhteysratkaisun vaatimukset

Etäyhteysratkaisun suunnittelussa ja toteuttamisessa ensimmäisenä vaiheena oli vaatimusten asettaminen ratkaisulle. Vaatimusten määrittelyn jälkeen laitevertailu on helpompaa, kun tiedetään, mihin ominaisuuksiin tulee kiinnittää huomiota. Seuraavaksi käydään läpi etäyhteysratkaisulle asetetut vaatimukset kohta kohdalta.

Lahti Precision Oy:n verkko asiakastehtaalla on erillään asiakkaan omasta verkosta. Lahti Precision Oy:n verkko sisältää mm. vaakaohjaimet, ohjelmoitavat logiikat ja niiden monitorointiin ja kontrollointiin käytettävät palvelinkoneet. Kuviossa 20 on esitetty esimerkki Lahti Precision Oy:n prosessiverkosta. Palvelinkoneiden virustorjuntaa ei pystytä aina pitämään ajan tasalla, joten prosessiverkon erottaminen asiakkaan verkosta on ensisijaisesti tietoturvakysymys.



KUVIO 20. Asiakastehtaan verkot

Yleiset vaatimukset

Laitteisto

Etäyhteysratkaisun toteuttamiseen vaadittavat tietoliikennelaitteet: laitteiden mallit ja niiden sijainnit verkoissa.

IP-protokolla

Etäyhteyksissä käytetään IP-protokollaa, joten myös laitteiden (sekä tietoliikennelaitteiden että tehdaslaitteiden) on sitä tuettava.

Yksilölliset IP-osoitteet LP:n asiakastehtaaseen toimittamille laitteille

Tehdaslaitteille on voitava määrittää yksilöllinen IP-osoite.

Laitevaatimukset

Haittaohjelmilta suojautuminen

Tietoliikennelaitteiden tarjoama tietoturva: palomuuri, virusturva, sisällön suodatin.

Varayhteys

Verkko-ongelmien varalta laitteissa tulisi olla mahdollisuus puhelinmodeemi/ISDN-yhteyden luomiseen.

Eri asiakkaiden yhteyksien erottaminen luotettavasti

Ei reititystä eri asiakkaiden VPN-tunnelien välillä, laitteen tulee erottaa VPN-tunnelit varmasti.

Lokitiedot

Etäyhteyslaitteen tulee kerätä lokitietoja tietoliikennetapahtumista. Lokitiedot tulee pystyä lähettämään toiselle koneelle (SysLog) tai sähköpostiin.

Etäyhteyslaitteen soveltuvuus tehdasolosuhteisiin

Etäyhteyslaitteen koteloinnin ja lämpötilakestävyyden tulee vastata asiakastehtaan olosuhteisiin. Laitteen virransyöttö tulee myös ottaa huomioon

Käytettävyys suhteutettuna käyttötarpeeseen

VPN-tunnelien käyttötarve ei ole korkea, joten tarvittaessa yhteyden avaamisen tulee olla sujuvaa ja ongelmatonta.

Laitekustannukset

Etäyhteyslaitteiden hinnoilla on suuri merkitys, kun laitteita hankitaan kymmeniä.

Etäyhteys tehtaaseen kotoa käsin

Työntekijöiden mahdollista saada VPN-yhteys asiakastehtaisiin myös muualta kuin työpaikalta. Vasteaika vikatilanteissa paranee huomattavasti.

Useita VPN-yhteyksiä/päällekkäiset verkko-osoitteet

Miten ratkaistaan päällekkäisten verkko-osoitteiden ongelma? Lahti Precision Oy:llä olevaan VPN-päätelaitteeseen terminoitavissa tunneleissa ei voi olla samoja verkko-osoitteita useissa eri asiakastehtaiden verkoissa. Ratkaisuna NAT tai jokin muu keino.

Keskitetty hallinta

Asiakastehtaissa olevien VPN-laitteiden hallinta keskitetysti. Kymmenien VPN-laitteiden hallinta ja monitorointi on hankalaa yksitellen, laitevalmistajalla ratkaisu keskitettyyn hallintaan toivottavaa.

VPN-tunnelien avaaminen ja sulkeminen

Millainen ratkaisu tunnelin avaamiseen ja sulkemiseen ja tapahtuuko Lahti Precision Oy:n päässä vai asiakastehtaan päässä?

4.4 Etäyhteysratkaisun laitevertailu

Laitevertailuun valittiin VPN-laitteita neljältä eri valmistajalta:

1. Siemens AG: Scalance S612 ja Scalance S613
2. Phoenix Contact: FL mGuard RS VPN
3. Innominate Security Technologies AG / Hirschmann: EAGLE mGuard
4. ZyXEL Communication Oy: ZyWALL 2 Plus.

Jokaisesta laitteesta löytyi hyvin informaatiota valmistajilta, joten vertailuun saatiin tarpeeksi materiaalia. VPN-tietojen osalta kaikki laitteet olivat lähes yhteneviä. IPsec oli tuettuna kaikissa, lisäksi molemmat mGuard-laitteet tukivat myös L2TP-tunneleita. Myös salaus- ja autentikointimenetelmät olivat kaikissa laitteissa samat. Salauksessa tuettiin DES, 3DES ja AES -menetelmiä ja autentikoinnissa MD5 ja SHA-1 -menetelmiä sekä esijaettuja avaimia sekä sertifikaatteja. Laitteiden hallinnan ja konfiguroinnin osalta tuli laitteiden välille eroavaisuuksia. Scalance-laitteiden hallinta ja konfigurointi vaati erillisen sovelluksen (Security Configuration Tool), kun muissa laitteissa hallinta ja konfigurointi onnistuu helpoimmillaan selaimella.

Varayhteyksiä laajakaistayhteyksien rinnalle tarjosivat ZyWALL 2 Plus ja FL mGuard RS VPN. ZyWALL 2 Plus -laitteessa on mahdollista ulkoisen modeemin avulla luoda VPN-modeemiyhteys ja FL mGuard RS VPN -laitteesta on tarjolla versio sisäänrakennetulla modeemilla/ISDN-modeemilla. Varayhteydet ovat tärkeitä etenkin sellaisissa maissa, joissa laajakaistayhteyksiä ei ole helposti saatavilla.

Käyttölämpötiloissa Scalance S613 oli omaa luokkaansa muihin verrattuna, mutta kaikkien käyttölämpötilat soveltuivat silti mainiosti tehdasolosuhteisiin, ZyWALL 2 Plus oli joukon ainoa, jossa on vain sähkönsyöttö pistorasiasta saatavilla. Laitevertailun ja seuraavissa kappaleissa läpikäytyjen laitetestien tulokset on esitetty taulukoituna liitteessä 1.

4.5 Etäyhteysratkaisun laitetestit

Jokaisesta laitemallista saatiin testiin laitepari, jonka välille VPN-tunneli luotiin. Siemens AG:lta saatiin yksi Scalance S612 ja yksi Scalance S613. Näissä ei kuitenkaan ollut muita eroavaisuuksia kuin Scalance S613 -laitteen suurempi VPN-tunnelien määrä ja laajempi lämpötilakestävyys.

Laitetestejä varten käytettiin erillistä ADSL-linjaa normaalin ulkoverkkoyhteyden lisäksi, jolloin VPN-tunnelien toimintaa voitiin testata siten, että paketit todella kiertävät ulkoverkon kautta. Tällöin VPN-laitteiden välille saatiin molempiin päihin reititin, kuten etäyhteysratkaisussa käytännössäkin tulee olemaan.

4.5.1 Scalance S612 ja S613

Scalance S612 ja S613 olivat ulkoisesti todella kestävän tuntuiset laitteet metallikuorineen ja suojauksineen. Laitteissa on kaksi paikkaa verkkokaapelille, ulkoverkon portti (WAN) ja sisäverkon portti (LAN). Työasema, jolla laitteiden konfigurointi tehtiin, kytkettiin LAN-porttiin, ja työasemaan asennettiin Siemensin konfigurointisovellus Security Configuration Tool. Laitteiden konfigurointi oli yksinkertaista, eikä VPN-tunnelin kuntoon saamiseen kulunut paljoa aikaa. Salaus- ja autentikointimenetelmiä pystyi itse muokkaamaan, joskin melko suppeasti. Scalancet muodostivat VPN-tunnelin automaattisesti heti, kun konfigurointi oli kunnossa. Asetuksissa oli myös ”Dead Peer Detection”, jonka päällä ollessa Scalance tarkkailee tunnelin vastapuolen tilaa, ja huomattuaan että vastapuoli ei enää vastaa, sulkee Scalance yhteyden ja neuvottelee VPN-tunnelin uudelleen. Scalancet sisältivät C-PLUG-tallennusmedian, johon konfigurointidata tallennettiin. Laitteen rikkoutuessa C-PLUG:in voi siirtää sellaisenaan toiseen laitteeseen, jolloin vikatilanteiden korjaus on todella nopeaa. Kokonaisuutena Scalancet olivat laadukkaita VPN-laitteita, mutta niiden ei katsottu soveltuvan Lahti Precision Oy:n tarpeisiin mm. tunnelien kontrolloinnin ja vajavaisten reititysmahdollisuuksien vuoksi. Lisäksi huomattavan korkea hinta vaikutti asiaan.

4.5.2 FL mGuard RS VPN

FL mGuard RS VPN oli ulkomuodoltaan samantyyppinen moduuli kuin Scalance S612/S613, joskin metallikuorien sijaan se oli muovikuorinen. FL mGuard RS VPN sisälsi kaksi verkkoliitäntää, LAN ja WAN. Työasema, jolla laitteiden konfiguraatio tehtiin, kytkettiin LAN-porttiin ja IP-osoite asetettiin vastaamaan laitteen verkkoaluetta. Nyt konfigurointi voitiin aloittaa selaimella. Selaimella tarvitsi vain kirjautua FL mGuard RS VPN -laitteen IP-osoitteeseen ja syöttää salasana, jonka jälkeen konfigurointinäkymä oli edessä. VPN-tunnelien konfigurointi oli tehty helpoksi, joten VPN-tunneli saatiin nopeasti kuntoon. FL mGuard RS VPN tuki VPN-päätelaitteiden autentikointia sertifikaattien avulla, joten laitteita varten piti luoda omat sertifikaatit. Sertifikaattien avulla voidaan toteuttaa turvallisempi etäyhteysratkaisu kuin esijaettujen avainten avulla. Sertifikaatit laitteisiin luotiin erillisellä sovelluksella.

VPN-tunnelien kontrollointia varten FL mGuard RS VPN tarjosi mahdollisuutena nk. VPN-kytkimen. FL mGuard RS VPN -laitteeseen voitiin kytkeä elektroninen kytkin, jolla voitiin kontrolloida VPN-tunnelin tilaa, eli VPN-tunneli voitiin avata ja sulkea kytkimestä. Tämän katsottiin olevan erinomainen ominaisuus asiakkaan näkökulmasta, koska asiakas voisi itse määritellä tunnelin tilan ilman kaapelien irroittamista laitteista. FL mGuard RS VPN tuki myös SysLog-menetelmää, eli laitteen lokitiedot voitiin lähettää ulkoiselle palvelimelle. Tätä varten testattiin muutamaa SysLog-sovellusta, ja toiminnon katsottiin toimivan kuten sen piti. Lokitiedot VPN-tunneleista ja palomuurista tulivat selkeästi SysLog-sovellukselle, jolla niistä voitiin saada tilastotietoja ja kaavioita. FL mGuard RS VPN oli kokonaisuutena erinomainen laite, joka oli melko lähellä tulla valituksi Lahti Precision Oy:n standardiksi etäyhteyslaitteeksi.

4.5.3 EAGLE mGuard

EAGLE mGuard on nimeä myöten lähes sama laite kuin FL mGuard RS VPN. EAGLE mGuard -laite oli ulkoisesti samanoloinen kuin FL mGuard RS VPN, ja

myös sen konfigurointi tapahtui selaimen avulla. VPN-tunnelien luonti oli jälleen vaivatonta, ja tunnelien toiminta saatiinkin testattua nopeasti. Myös EAGLE mGuard -laite käytti päätelaitteiden autentikointiin sertifikaatteja, jotka luotiin erillisellä sovelluksella. Toiminnoiltaan ja ominaisuuksiltaan EAGLE mGuard vastasi siis melko pitkälle FL mGuard RS VPN -laitetta. Taulukossa 1 on vertailtu laitteita niiden ominaisuuksien osalta, joille ei ollut vastaavutta.

TAULUKKO 1. FL mGuard RS VPN ja EAGLE mGuard

Ominaisuus	FL mGuard RS VPN	EAGLE mGuard
hardware clock	kyllä	ei
"VPN-kytkin"	kyllä	ei
IKE Fragmentation	kyllä	ei
IPsec MTU	kyllä	ei
Hub-and-spoke eli reititys VPN-tunnelien välillä	kyllä	ei
Ping Check, IKE Ping	kyllä	ei
USB-liitäntä (a USB port that supports a configuration flash adapter and remote administration via the Internet.)	ei	kyllä
	~950€	~720€

Laitteen sisäistä kelloa ei katsottu kovin tärkeäksi, sillä VPN-laite on yhteydessä ulkoverkkoon, jolloin ajan päivittäminen aikapalvelimelta on mahdollista. VPN-kytkimen puute oli suurempi menetys, sillä sen katsottiin olevan yksi FL mGuard RS VPN -laitteen parhaista ominaisuuksista. IKE Fragmentation ja IPsec MTU olivat ainakin testausvaiheessa tarpeettomia: niistä on apua ylisuurien sertifikaattien ja UDP-pakettien kanssa, jotka FL mGuard RS VPN voisi pilkkoa ennen lähetystä. Reititystä VPN-tunnelien välillä ei tarvittu, koska asiakkaiden verkot haluttiin muutenkin pitää erillään toisistaan. Ping Check ja IKE Ping ovat pieni apu testausvaiheessa, kun varmistetaan tunnelin toimivuutta tai ongelmia siinä. EAGLE mGuard sisälsi USB-portin, johon oli saatavilla konfigurointiadapteri. Konfigurointiadapteriin voitiin tehdä valmis konfiguraatio ja liitettäessä se EAGLE mGuard -laitteeseen latautuisi konfiguraatio automaattisesti. Kokonaisuudessaan erot ominaisuuksissa eivät olleet laitteiden hintaeron arvoisia, eli EAGLE mGuard oli parempi vaihtoehto laitekaksikosta.

4.5.4 ZyWALL 2 Plus

ZyWALL 2 Plus erosi edellä testatuista laitteista ensisijaisesti ulkomuotonsa osalta. ZyWALL 2 Plus on ensisijaisesti toimistokäyttöön tarkoitettu laite eikä teollisuusolosuhteisiin, kuten edelliset laitteet. ZyWALL 2 Plus sisälsi myös useampia portteja kuin muut laitteet: 1 WAN-portti ja 4 LAN-porttia, joiden lisäksi ZyWALL 2 Plus -laitteessa oli konsoliportti ja Dial Backup -portti modeemiyhteyttä varten. ZyWALL 2 Plus -laitteen konfigurointi tapahtui myös selaimella. Selainkäyttöliittymä oli selkeästi jaoteltu, ja valikoiden alta löytyi kaikki tarvittava. VPN-tunnelin konfigurointi onnistui jälleen ongelmitta. Salausasetukset sisälsivät samat menetelmät kuin edellä testatut laitteet, ja päätelaitteiden autentikointi tapahtui sertifikaattien avulla.

ZyWALL 2 Plus yllätti helppokäyttöisyydellään ja kattavilla ominaisuuksillaan. VPN-tunnelien tilaa pystyi valvomaan erikseen ja lokitiedoista kävi hyvin ilmi, mistä ongelmat johtuivat vikatilanteissa. Tilallinen palomuuri katsottiin myös enemmän kuin riittäväksi etäyhteysratkaisun tarpeisiin. ZyXEL tarjoaa laitteille myös keskitettyä hallintaa Vantage CNM -hallintajärjestelmän muodossa. Vantage CNM -järjestelmää ei tämän opinnäytetyöprojektin aikana päästy testaamaan, sillä sen hankintaa ei katsottu vielä tarpeelliseksi. Hintansa osalta ZyWALL 2 Plus oli ylivoimaisesti edullisin vertailun laitteista.

4.5.5 Laitevertailun ja -testien tulokset

Vertailun ja tehtyjen testien jälkeen standardiksi etäyhteyslaitteeksi valittiin ZyXEL ZyWALL 2 Plus. ZyWALL 2 Plus sisälsi lähes kaikki ominaisuudet, mitä muutkin testissä olevat laitteet ja oli silti lähes neljä kertaa edullisempi vaihtoehto kustannusmielessä kuin seuraavaksi halvin laite, Hirschmann Eagle. ZyWALL 2 Plus vastasi hyvin kappaleessa 4.3 esitettyihin vaatimuksiin etäyhteysratkaisulle.

Taulukossa 2 on kuvattu testattujen laitteiden vastaavuudet vaatimuksiin. Scalance S612 ja S613 -laitteita taulukossa ei ole, koska ne katsottiin jo aikaisessa vaiheessa sopimattomiksi etäyhteysratkaisun toteuttamiseen.

TAULUKKO 2. Laitteiden vastaavuudet vaatimuksiin

Laite	**Haittaohjelmilta suojautuminen**
Phoenix	palomuuri, lisenssillä myös virusturva
Hirschmann	palomuuri, lisenssillä myös virusturva
Zyxel	palomuuri, sisällönsuodatus
	Varayhteys
Phoenix	modeemi/ISDN-varayhteys (RS VPN Analog tai RS VPN ISDN)
Hirschmann	ei ole
Zyxel	Dial Backup
	Eri asiakkaiden yhteyksien erottaminen luotettavasti
Phoenix	yhteydet vain sertifikaattiparien välillä, mGuard ei reitittä (oletuksena) dataa VPN-tunnelien välillä
Hirschmann	yhteydet vain sertifikaattiparien välillä, mGuard ei reitittä (oletuksena) dataa VPN-tunnelien välillä
Zyxel	yhteydet vain sertifikaattiparien välillä, VPN-tunnelien liikennettä ei reititetä keskenään (palomuurisäännöt)
	Lokitiedot
Phoenix	Lokissa yleiset tapahtumat, palomuuritapahtumat ja VPN-tapahtumat. mGuard tallentaa lokin sisäisesti, pysyy tallessa kunnes virrat sammutetaan, SysLog toimii.
Hirschmann	Lokissa yleiset tapahtumat, palomuuritapahtumat ja VPN-tapahtumat. mGuard tallentaa lokin sisäisesti, pysyy tallessa kunnes virrat sammutetaan, SysLog toimii
Zyxel	Lokissa kaikki tapahtumat, voi filtteröidä, lokit voi lähettää sähköpostiin, SysLog toimii
	Etäyhteyslaitteen soveltuvuus tehdasolosuhteisiin
Phoenix	Lämpötila 0℃-60℃, reduntanttinen 12V tai 24V virr ansyöttö, DIN-kiskolle asennus, IP 20
Hirschmann	Lämpötila 0℃-60℃, reduntanttinen 12V tai 24V virr ansyöttö, DIN-kiskolle asennus, IP 20
Zyxel	Lämpötila 0℃-50℃, 12VDC
	Käytettävyys suhteutettuna käyttötarpeeseen
Phoenix	oikein konfiguroituna yhteyden avaus nappia painamalla
Hirschmann	yhteys aina päällä, muuten vaatii admin-oikeudet (tai url-osoitteella, admin)
Zyxel	tunnelin avaaminen/sulkeminen kuvaketta klikkaamalla
	Laitekustannukset
Phoenix	950 €
Hirschmann	720 €
Zyxel	138,80 €
	Etäyhteys tehtaaseen kotoa käsin
Phoenix	sertifikaattien avulla onnistuu esimerkiksi Windows-clientin avulla
Hirschmann	sertifikaattien avulla onnistuu esimerkiksi Windows-clientin avulla
Zyxel	onnistuu: ZyXEL USG 300 (SSL VPN) -> ZyWALL 2 Plus (IPsec VPN)
	Useita VPN-yhteyksiä/päällekkäiset verkko-osoitteet
Phoenix	virtual NAT / 1:1 NAT
Hirschmann	virtual NAT / 1:1 NAT

Zyxel	virtual NAT / 1:1 NAT
	Keskitetty hallinta
Phoenix	Innominate Device Manager
Hirschmann	Innominate Device Manager
Zyxel	Vantage CNM
	VPN-tunnelien avaaminen ja sulkeminen
Phoenix	VPN-kytkimellä, webbihallinnan kautta/url-osoitteen avulla - vaatii admin-oikeudet
Hirschmann	webbihallinnan kautta/url-osoitteen avulla - vaatii admin-oikeudet
Zyxel	webbiliittymä, listasta kuvaketta klikkamalla auki/kiinni, skriptit (CLI/SSH)

ZyWALL 2 Plus oli vertailunelikon ainoa ensisijaisesti toimistokäyttöön tarkoitettu etäyhteyslaite. ZyWALL 2 Plus on siis laitteena pöytämalli ja sen kotelointi ja ulkomuoto erosi muista vertailun laitteista huomattavasti. Muut kolme etäyhteyslaitetta olivat tehdasolosuhteisiin suunniteltuja ja siten ulkomuodoltaan melko yhteneviä. Lisäksi muissa laitteissa oli kiskokiinnitysmahdollisuus, joten ne olisivat sopineet ongelmitta muiden laitteiden rinnalle sähkökaappiin, johon etäyhteyslaite tullaan aina sijoittamaan. ZyWALL 2 Plus -laitetta varten jouduttiin sähkökaappiin suunnittelemaan erillinen kisko, johon ZyWALL 2 Plus voidaan ripustaa ja kiinnittää. Lisäksi ZyWALL 2 Plus käyttää normaalia 12V muuntajaa, joka vaatii pistorasiapaikan. Pistorasiapaikkaa sähkökaapissa ei aina ole, joten sähkönsyöttöä varten hankittiin erillinen kiskoon kiinnitettävä Phoenix Contact -valmistajan virtalähde, joka kytketään ZyWALL 2 Plus -laitteeseen. Edellä kuvattuja toimenpiteitä varten tehtiin ZyWALL 2 Plus -laitteelle asennusohje, jonka mukaan tehdään sen asennus, kiinnitys ja kytkentä sähkökaappiin.

4.6 Pilottihanke

Pilottihanke toteutettiin Lahti Precision Oy:n ja Turkissa sijaitsevan asiakastehtaan välillä. Tämä tapahtui melko pian sen jälkeen, kun ZyWALL 2 Plus oli valittu Lahti Precision Oy:n standardiksi etäyhteyslaitteeksi. Pilottihankkeen VPN-tunneli toteutettiin kahden ZyWALL 2 Plus -laitteen välillä. Molemmat laitteet konfiguroitiin valmiiksi Lahti Precision Oy:llä, ja VPN-tunnelin toiminta

varmistettiin testaamalla. Toinen laite lähti ohjaussuunnitteluinsinöörin matkassa Turkkiin ja toinen jäi Lahti Precision Oy:n tiloihin.

Turkissa ZyWALL 2 Plus sijoitettiin asiakkaan verkon ja Lahti Precision Oy:n prosessiverkon väliin siltaavassa tilassa. ZyWALL 2 Plus täytyi laittaa siltaavaan tilaan, koska molemmat verkot kuuluivat samaan aliverkkoon, eivätkä verkkojen IP-osoitteet menneet sopivasti aliverkon maskien mukaan (eli asiakkaan verkko-osoitteet olisivat olleet aliverkkoalueen alkupäästä ja Lahti Precision Oy:n aliverkkoalueen loppupäästä, tai toisinpäin), joten niiden välille ei voitu laittaa reititintä. Tämä ei kuitenkaan ollut ongelma VPN-tunnelin muodostuksen kannalta.

ZyWALL 2 Plus oli siis nyt oikealla paikallaan, ja VPN-tunnelin testaus voitiin aloittaa. VPN-tunneli ei muodostunutkaan ongelmitta kuten sen olisi pitänyt, joten alkoi vianetsintä ja konfigurointien tutkiminen. Myöskään internetiin ei päässyt enää Lahti Precision Oy:n prosessiverkosta, kun ZyWALL 2 Plus laitettiin verkkojen väliin. Tämä sai jo epäilemään muutakin kuin konfigurointivirhettä, koska Lahdessa tehdyissä testeissä kaikki oli toiminut hyvin eikä palomuurissa oltu erikseen kielletty internetliikennettä. Molempien laitteiden lokitietoja ja konfigurointeja vertailtiin, mutta loppujen lopuksi syynä oli väärässä portissa ollut ethernet-kaapeli. Kaapelin siirron jälkeen VPN-tunneli muodostuikin ongelmitta, ja myös Internetin käyttö onnistui ZyWALL 2 Plus -laitteen takaa. VPN-tunnelin muodostuminen ei kuitenkaan vielä taannut ongelmien loppumista. Vaikka VPN-tunneli oli muodostunut, ei siinä tuntunut kulkevan yhtään liikennettä. Tämä ratkaistiin laittamalla Turkin ZyWALL 2 Plus pingaamaan Lahden ZyWALL 2 Plus -laitetta. Kyseinen ominaisuus on ZyWALL 2 Plus -laitteessa nimellä ”Check IPsec Tunnel Connectivity”, johon määritellään pingattava IP-osoite. Konfigurointimuutoksen jälkeen VPN-tunneli oli toiminnassa, ja myös liikenne kulki siinä ongelmitta. Johtopäätöksenä tästä oli se, että koska Turkin ZyWALL 2 Plus oli VPN-tunnelin muodostuksen aloittaja eli initiator, täytyy sen lähettää ensin jonkinlaista liikennettä tunneliin, ennen kuin tunnelin liikenne on kaksisuuntaista.

Nyt Lahti Precision Oy:n ja Turkin asiakastehtaan välillä oli VPN-tunneli toiminnassa, joten sovellusten ja monitoroinnin toimivuutta VPN-tunnelin läpi voitiin testata. Ohjelmoitaviin logiikoihin saatiinkin yhteys nopeasti ja myös tiedonsiirtonopeuden vaikutukset käytettävyyteen yllättivät positiivisesti. Vertailukohtanahan olivat puhelinmodeemeilla toteutetut etäyhteydet. Myös prosessiverkon palvelinkoneisiin saatiin yhteys, ja niitä voitiin monitoroida VPN-tunnelin läpi. ZyWALL 2 Plus -laitteen konfigurointi ja lokien luku onnistui myös mainiosti VPN-tunnelin yli.

Pilottihankkeessa esiin tulleet ongelmat ja tehdyt testit olivat arvokkaita etäyhteysratkaisun tulevaisuuden kannalta. VPN-tunnelin toiminnasta saatiin myös hyviä tuloksia ja kokemuksia, joten kokonaisuutena pilottihanke katsottiin onnistuneeksi ja hyödylliseksi projektille.

4.7 ZyWALL USG 300

Projektissa seuraavana oli Lahti Precision Oy:lle sopivan VPN-laitteen hankinta. Lahti Precision Oy:lle tarvittiin siis VPN-laite, johon kymmenet VPN-tunnelit muodostetaan ja jossa riittää tiedonsiirtokapasiteettia ja ominaisuuksia kymmeniä etäyhteyksiä varten. Lisäksi laitteesta oli toivottavaa löytyä SSL VPN -ominaisuus, jolloin etäyhteyksiä olisi mahdollista käyttää mistä vain. Lyhyen tutkimisen ja vertailun jälkeen ZyXEL:in mallistosta löytyikin ominaisuuksiltaan sopiva laite: ZyWALL USG 300.

ZyWALL USG 300 sisältää tuen sekä IPsec että SSL VPN -tunneleille. Yhtäaikaisia IPsec VPN -tunneleita voi olla maksimissaan 200 ja yhtäaikaisia SSL VPN -tunneleita maksimissaan kymmenen. Etäyhteyksien käyttöaste huomioon ottaen määrät riittivät enemmän kuin hyvin. Muita tärkeitä ominaisuuksia ZyWALL USG 300:ssa olivat mm. RADIUS-tietokannan liittäminen laitteeseen (etäyhteyksien käyttäjät tunnistetaan RADIUS-palvelimen avulla) ja laajat reitityksen konfigurointimahdollisuudet. Lisäksi ZyWALL USG 300 oli hyvin edullinen laite ottaen huomioon sen tarjoamat ominaisuudet.

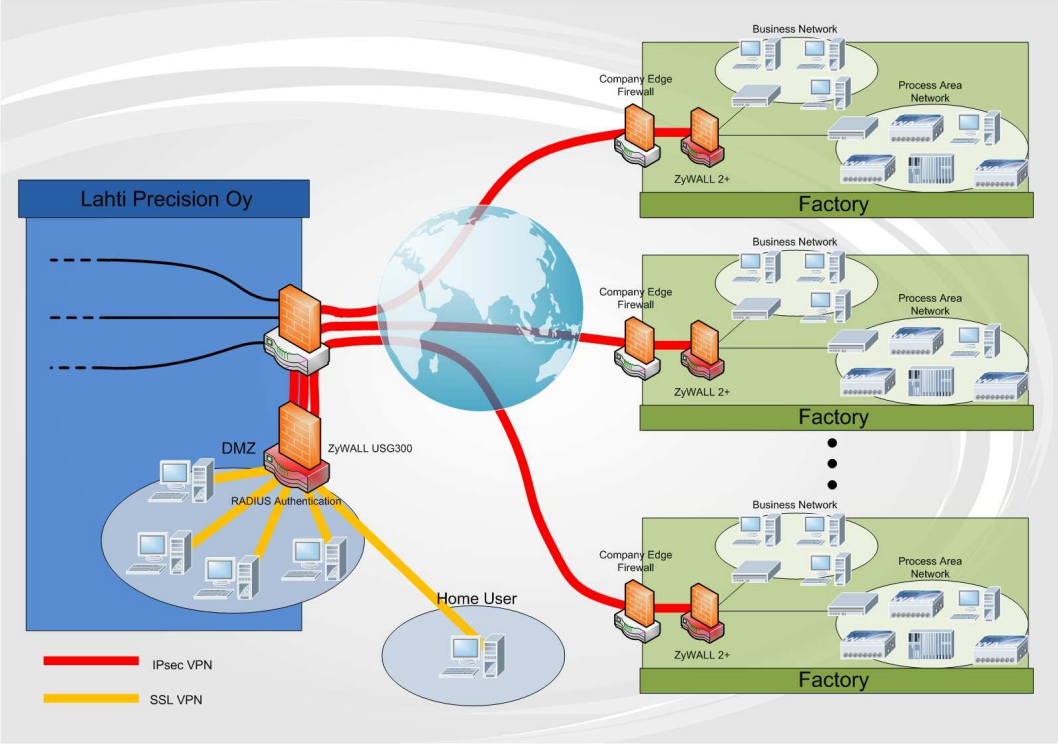
ZyWALL USG 300:n SSL VPN oli yksi tärkeimmistä syistä, miksi laitteeseen päädyttiin. Laitteella on mahdollista muodostaa kahdenlaisia SSL VPN -tunneleita. Ensimmäisenä vaihtoehtona on normaali SSL VPN, jolle voidaan määritellä saatavilla olevat sovellukset ja tiedostot ja jonka toiminta on kuin minkä tahansa muun SSL VPN -tunnelin, eli tunneli ei ulotu verkkotasolle asti. Toisena vaihtoehtona ZyWALL USG 300 tarjoaa SSL VPN -tunnelin, jota ZyXEL kutsuu nimellä SecuExtender (Full Tunnel Mode). SecuExtender laajentaa SSL VPN -tunnelin verkkotasolle, jolloin SSL VPN -tunneli vastaa käytännössä IPsec VPN -tunnelia. Kirjauduttaessa SSL VPN:ään ZyWALL USG 300 lisää käyttäjän koneelle virtuaaliadapterin, jolle on määritelty IP-osoite ZyWALL USG 300:n konfiguroinnissa. Lisäksi ZyWALL USG 300 lisää konfiguroinnissa määritellyt verkot SSL VPN:ään kirjautuvan koneen reititystauluun. Määritellyille verkoille lähtevien pakettien kohteena on ZyWALL USG 300:n SSL-liitäntä, ja reitityssääntöjen metric-arvo on 2, minkä vuoksi kone lähettää kaikki SSL VPN -verkkoihin lähtevät paketit ZyWALL USG 300:n SSL-liitäntään, josta ZyWALL USG 300 reitittää paketit edelleen reitityssääntöjen mukaan. Pieni metric-arvo takaa, että määriteltyihin verkkoihin lähtevät paketit menevät varmasti ZyWALL USG 300:n kautta. SecuExtender tarjoaa siis verkkotason VPN-tunnelin ilman erillisiä asiakasohjelmistoja, joita IPsec VPN -tunnelissa vaadittaisiin.

ZyWALL USG 300 sijoitettiin Lahti Precision Oy:n palomuurin DMZ-alueelle. ZyWALL USG 300 sai oman kiinteän julkisen IP-osoitteen, johon asiakastehtaissa olevat ZyWALL 2 Plus -laitteet ottavat yhteyden. Ensimmäiseksi ZyWALL USG 300 -laitteeseen tehtiin peruskonfiguraatio, eli IP-osoitteet ja reititystiedot laitettiin kuntoon, ja palomuuriin tehtiin perussäännöt. Lisäksi määriteltiin käytettävä RADIUS-palvelin ja siihen liittyvät asetukset.

IPsec VPN -asetusten konfigurointi oli suurimmilta osin samanlaista kuin ZyWALL 2 Plus -laitteessa. IPsec VPN -tunneleissa tullaan käyttämään samoja salausasetuksia kuin aikaisemmin tehdyissä testeissä ja pilottihankkeessa. Tunnistautuminen laitteiden välillä on edelleen sertifikaattipohjaista, eli ZyWALL USG 300 -laitteelle luotiin oma sertifikaatti erillisellä sovelluksella. Lisäksi

ZyWALL USG 300 -laitteeseen täytyi luoda IPsec VPN -tunneleihin liittyvät reitityssäännöt erikseen, jotta laite osaa reitittää paketit oikeisiin IPsec VPN -tunneleihin.

Seuraavaksi konfiguroitiin ZyWALL USG 300 -laitteen SSL VPN -asetuksia. Ideana oli käyttää ZyWALL USG 300:n SecuExtender SSL-tunnelia, jolloin SSL VPN-käyttäjien liikenne voidaan reitittää muodostettuihin IPsec VPN -tunneleihin. IPsec VPN -tunneli on siis ZyWALL USG 300:n ja asiakastehtaassa sijaitsevan ZyWALL 2 Plus -laitteen välillä, ja SSL VPN -tunneli luodaan käyttäjän ja ZyWALL USG 300 -laitteen välille. Tämä mahdollistaa etäyhteyksien käyttämisen ilman tarvetta olla kiinni ZyWALL USG 300:n LAN-liitännässä tai aliverkossa, joka toimii IPsec VPN -tunnelin toisena päätepisteenä. Edellä määritelty verkkotopologia on esitetty kuviossa 21.



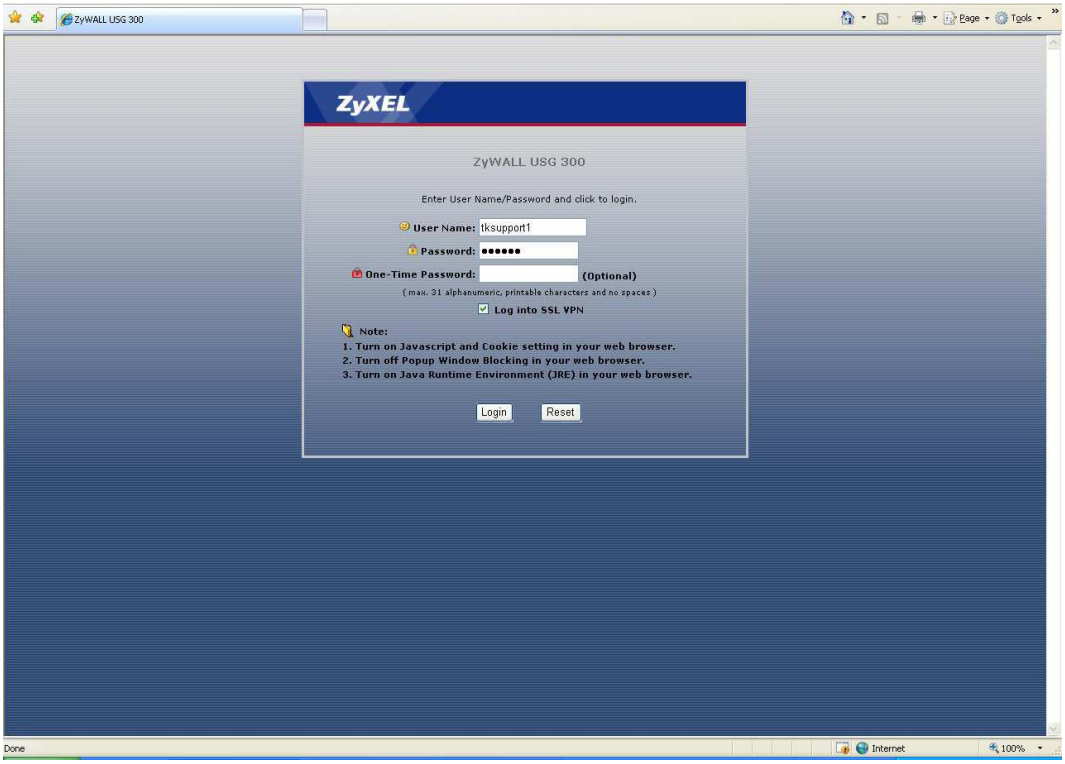
KUVIO 21. VPN-tunnelit

SSL VPN -käyttäjät tunnistetaan RADIUS-palvelimen avulla. RADIUS-palvelimen asetukset konfiguroitiin ZyWALL USG 300:n, ja laitteiden välisen kommunikoinnin toiminta varmistettiin. SSL VPN -käyttäjät syöttävät

kirjautuessaan käyttäjätunnuksensa ja kertakäyttösalasanan, jotka ZyWALL USG 300 lähettää RADIUS-palvelimelle, joka tunnistaa käyttäjät. SSL VPN -käyttäjät lisätään USG 300:n käyttäjätyypillä ”Ext-User”. Ext-User -tyyppisten käyttäjien tunnistamiseen ZyWALL USG 300 käyttää ulkoisia palvelimia, kuten RADIUS tai LDAP.

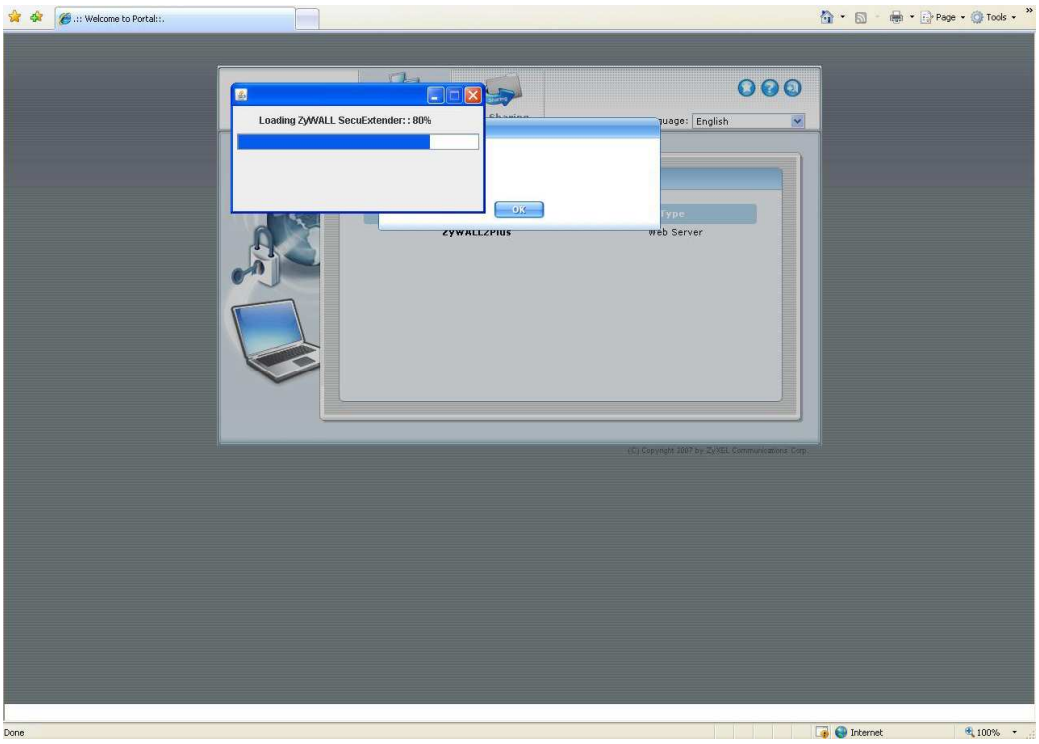
Itse SSL VPN -asetuksien konfiguroinnissa ZyWALL USG 300 käyttää nk. SSL-yhteyspolitiikkoja (SSL Access Policy). Etäyhteyksien käyttäjille määriteltiin uusi yhteyspolitiikka nimellä ”RemoteSupportService”. Tähän yhteyspolitiikkaan lisätään käyttäjät, joille sallitaan etäyhteyksien käyttö. Jokaiselle käyttäjälle ei siis tarvitse tehdä erillistä yhteyspolitiikkaa. Yhteyspolitiikan asetuksissa voidaan määritellä myös käyttäjille näkyvät SSL-sovellukset, mutta näille ei ollut tarvetta vielä. Tärkeintä oli määritellä SSL VPN -käyttäjien verkkotason asetukset, jotta SecuExtender voidaan ottaa käyttöön. SSL VPN -käyttäjille määriteltiin oma osoitealue SSLpool, josta käyttäjille jaetaan IP-osoitteet. DNS-palvelimena toimii itse ZyWALL USG 300. Lisäksi määritellään, mihin verkkoihin SSL VPN -käyttäjillä on oikeus liikennöidä; tähän määriteltiin 10.10.0.0/16, jolloin käyttäjillä on oikeus liikennöidä kaikkiin asiakastehtaisiin. Nyt SSL VPN -asetukset oli konfiguroitu, ja määritellyt käyttäjät pääsivät kirjautuessaan ZyWALL USG 300 -laitteeseen liikennöimään asiakastehtaisiin.

Seuraavassa käydään läpi SSL VPN SecuExtender -tunneliin kirjautuminen ja siinä tapahtuvat prosessit. ZyWALL USG 300:n kirjautumisikkuna avautuu, kun selaimella mennään laitteelle määritettyyn IP-osoitteeseen. Kirjautumisikkuna on esitetty kuviossa 22.



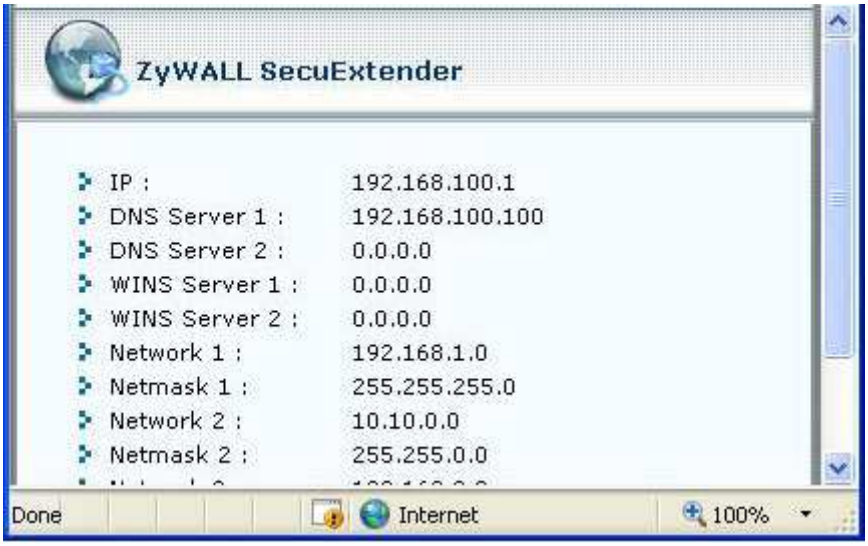
KUVIO 22. Kirjautuminen

Käyttäjä syöttää kirjautumisikkunaan käyttäjätunnuksensa ja kertakäyttösalasanan. Käyttäjän on muistettava laittaa myös ruksi ”Log into SSL VPN” -kohtaan, jotta käyttäjä kirjautuu nimenomaan SSL VPN -tunneliin eikä itse ZyWALL USG 300 -laitteeseen. Login-nappia klikkaamalla ZyWALL USG 300 aloittaa SecuExtenderin lataamisen käyttäjän työasemalle. Tässä vaiheessa työasemalle ladataan kevyt Java-sovellus, joka huolehtii SSL VPN -tunnelin luomisesta ja ylläpidosta. Kuviossa 23 on esitetty SecuExtenderin latausnäkymä.



KUVIO 23. SecuExtenderin latautuminen

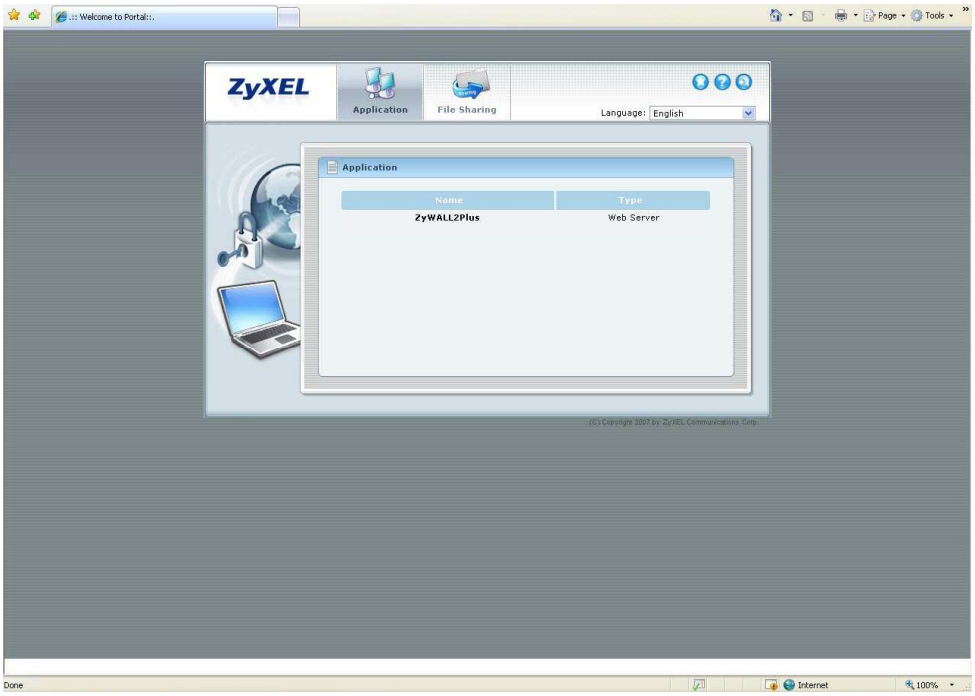
Latauduttuaan SecuExtender esittää käyttäjälle erillisessä ikkunassa (Kuvio 24) IP-osoitetiedot: virtuaaliadapterille määritellyn IP-osoitteen, DNS-palvelimet ja ne verkot, joihin käyttäjällä on oikeus päästä.



KUVIO 24. SecuExtenderiin määritellyt IP-osoitteet ja verkot

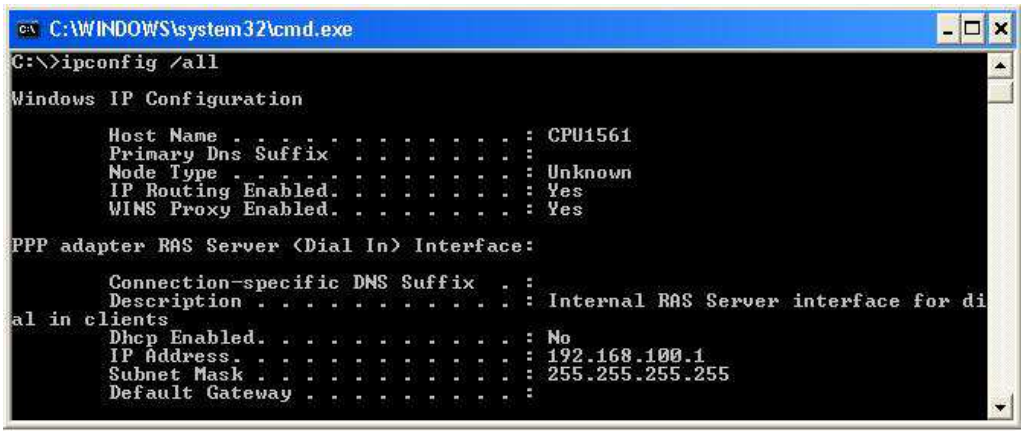
Nyt SSL VPN SecuExtender -tunneli on luotu, ja käyttäjälle on näkyvissä portaalinäkymä (Kuvio 25). Portaalinäkymässä SecuExtender -käyttäjälle voidaan

määritellä sovelluksia, kuten normaalille SSL VPN -käyttäjälle. SecuExtender toimii kuitenkin verkkotasolla, joten portaalinäkymää ei tarvita ollenkaan, kun ollaan yhteydessä aikaisemmin määriteltyihin verkkoihin.



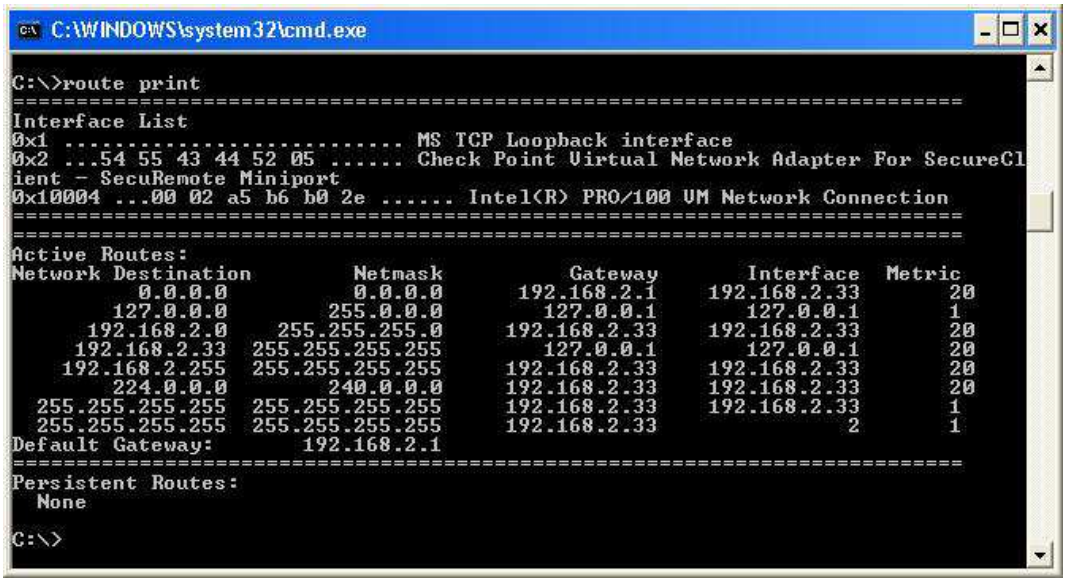
KUVIO 25. Portaalinäkymä

SecuExtender siis luo käyttäjän työasemalle virtuaaliadapterin (Kuvio 26), joka toimii linkkinä työaseman ja ZyWALL USG 300:n välillä. Virtuaaliadapteri näkyy käyttäjälle muiden verkkokorttien yhteydessä.

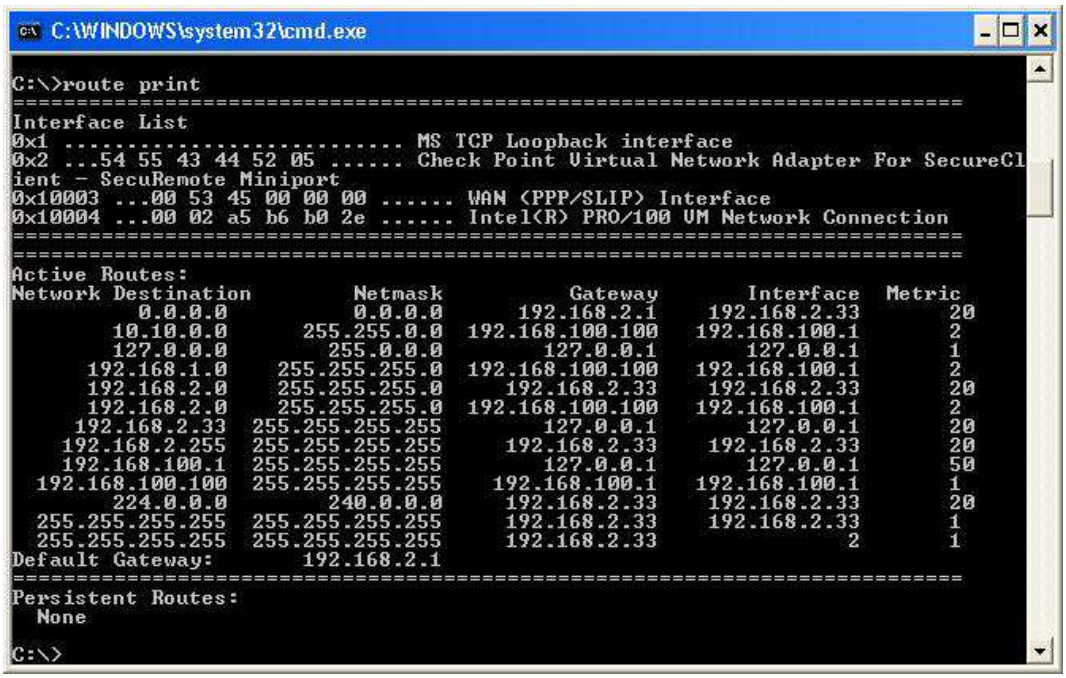


KUVIO 26. SecuExtenderin luoma virtuaaliadapteri

Kuvioissa 27 ja 28 on esitetty käyttäjän työaseman reititystaulut ennen ja jälkeen SecuExtenderin latauksen. SecuExtender siis lisää automattisesti konfiguroinnissa määritellyt verkot työaseman reititystauluun. Näiden verkkojen gatewaynä toimii ZyWALL USG 300 -laitteen SSL VPN -liitynnälle annettu IP-osoite. Kuten kuviosta 28 voidaan todeta, lisätään uudet reitit reititystauluun alhaisella metric-arvolla, joka takaa, että ne ovat suositeltuja reittejä määriteltyihin verkkoihin. Esimerkiksi reitti verkkoon 192.168.2.0/24 oli jo aikaisemmin olemassa isäntäkoneessa metric-arvolla 20, mutta koska SecuExtenderiin on myös määritelty verkko 192.168.2.0/24, näkyy se reititystaulussa myös pienemmällä metric-arvolla 2. Näin ollen isäntäkone lähettääkin kyseiseen verkkoon lähtevät paketit ZyWALL USG 300 -laitteelle, eikä gateway-osoitteelle 192.168.2.33.

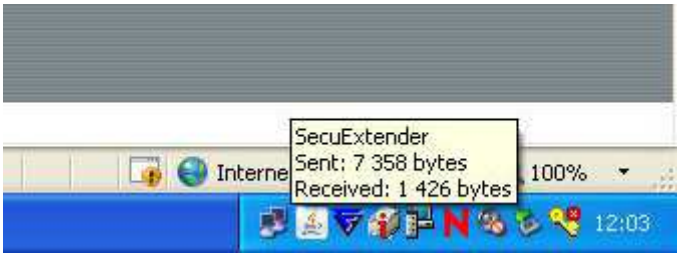


KUVIO 27. Isäntäkoneen reititystaulu ennen SecuExtenderin latausta



KUVIO 28. Isäntäkoneen reititystaulu SecuExtenderin latauksen jälkeen

SecuExtenderin ollessa päällä ja toiminnassa näkyy kuviossa 29 esitetty kuvake, jossa on kaksi tietokonetta Windowsin tehtäväpalkissa. Viemällä hiiren kuvakkeen päälle voi käyttäjä nähdä SecuExtenderin lähettämät ja vastaanottamat liikennemäärät.



KUVIO 29. SecuExtenderin lähettämät ja vastaanottamat liikennemäärät

4.8 Aliverkotus

Seuraavaksi ongelmaksi etäyhteysratkaisussa muodostuivat käytetyt aliverkot. Jokaisessa projektissa oli tapana käyttää samaa aliverkkoa, joka aiheutti ongelman IPsec VPN:n kannalta. Tässä tilanteessa laitteita konfiguroitaessa jokaiselle VPN-tunnelille olisi määriteltävä samat aliverkot tunnelin molempiin päihin kaikissa

projekteissa. Tämä aiheuttaisi VPN-tunneleiden käytettävyyteen vakavia puutteita, koska vain yksi VPN-tunneli voisi olla kerrallaan päällä.

Ongelman ratkaisua varten pidettiin palaveri, jossa päätettiin ottaa käyttöön uudet aliverkot. Jokaiselle projektille tultaisiin antamaan aliverkko verkkoavaruudesta 10.10.0.0/16. Jokainen projekti saisi siis yhden 10.10.x.0/24 -osoiteavaruuden, jossa x on juokseva numero projektin mukaan. Tällä ratkaistaan päällekkäisten osoitteiden ongelmat, ja jokaisella maailmalla olevalla laitteella on yksilöllinen IP-osoite.

Uusien aliverkkojen takia myös Lahti Precision Oy:n testiverkkoon piti tehdä muutoksia. Testiverkossa prosessialueen laitteiden toiminta testataan ja simuloidaan ennen niiden toimittamista asiakastehtaaseen. Tähän mennessä testiverkolla oli ollut aina sama aliverkkoalue, jossa oli vain yksi gateway-osoite. Kun uusi 10.10.0.0/16 -osoiteavaruus otettiin käyttöön, gateway-osoitteiden määrä aiheutti ongelman. Jokaisen projektin laitteilla on oma gateway, toisin sanoen gateway-osoitteita on yhteensä 255. Testiverkkoon täytyi siis saada sellainen laite, johon on mahdollista konfiguroida 255 IP-osoitetta samalle liitännälle.

Riittävä määrä IP-osoitteita oli mahdollista asettaa esimerkiksi Ciscon valmistamissa reitittimissä sekä Linux-koneissa, joissa verkkokortille voidaan määrittää satoja IP-osoitteita. Tähän tehtävään katsottiin parhaimmaksi vaihtoehdoksi Linux-palvelin. Linux-palvelin oli ilmainen ja mahdollinen asentaa vähän vanhempaan työasemaan, joten kustannusnäkökulmasta Linux-palvelin oli ylivertainen vaihtoehto. Linux-palvelin on myös vakaa, toimintavarma ja osaavissa käsissä monipuolinen. Palvelimeksi valittiin Ubuntu Server 8.04 (Hardy Heron), joka ladattiin ja asennettiin vanhaan työasemaan. Työasemaan laitettiin kaksi verkkokorttia, joista toinen toimii testiverkon gatewaynä ja toinen yhdistettiin Lahti Precision Oy:n palomuuriin. Ubuntu Serverille tehtiin vaadittavat konfiguraatiot, ja toiselle verkkokortille asetettiin kaikki testiverkon gateway-osoitteet. Nyt Ubuntu Server toimi reitittimenä testiverkon ja Lahti Precision Oy:n sisäverkon välillä. Testiverkossa laitteisiin voitiin asettaa IP-osoitteet ja gatewayt ilman ongelmia, koska Ubuntu Server toimi jokaisen

10.10.x.0/24 -verkon gatewaynä. Näin laitteet voidaan siirtää suoraan testiverkosta asiakastehtaille ilman IP-osoitteiden tai gateway-osoitteiden muunnoksia.

4.9 Seuraava etäyhteys

Seuraava etäyhteys toteutettiin Lahti Precision Oy:n ja Ukrainassa sijaitsevan asiakastehtaan välillä. Nyt LP:n tiloissa oli juuri hankittu ZyWALL USG 300, joten etäyhteys voitiin luoda ZyWALL USG 300:n ja ZyWALL 2 Plus -laitteen välille, kuten lopullisessa ratkaisussa on tarkoituskin. Pilottihankkeessahan etäyhteys toteutettiin kahden ZyWALL 2 Plus -laitteen välillä.

ZyWALL 2 Plus -laitteeseen konfiguroitiin IPsec-asetukset ja muut asetukset kuntoon, ja laite lähti ohjaussuunnitteluinsinöörin matkassa Ukrainaan. ZyWALL USG 300 -laitteeseen konfiguroitiin vastaavasti IPsec-asetukset, ja VPN-tunnelin toiminta testattiin ennen ZyWALL 2 Plus -laitteen matkalle lähtöä.

Ukrainassa oli vielä käytössä vanha aliverkko Lahti Precicion Oy:n prosessiverkossa, joten kaikkien prosessiverkon laitteiden IP-osoitteet oli muutettava vastaamaan määriteltyä 10.10.x.0/24 -verkkoa. Tämän jälkeen ZyWALL 2 Plus -laite sijoitettiin reitittävässä tilassa prosessiverkon ja asiakkaan verkon välille. ZyWALL 2 Plus -laite ottikin heti kytkettyään yhteyden Lahdessa sijaitsevaan ZyWALL USG 300 -laitteeseen, mutta laitteiden välinen tunnistautuminen ei mennyt läpi. Tunnistautumisongelman syyksi paljastui ZyWALL 2 Plus -laitteen sertifikaatti, jonka ZyWALL 2 Plus ei katsonut olevan vielä voimassa. ZyWALL 2 Plus ei ollut saanut päivitettyä aika- ja päivämääräasetuksiaan, kun se oli kytketty verkkoon, joten laite oli oletusasetuksilla vuodessa 2000. Aika- ja päivämääräasetusten päivittämisen jälkeen tunnistautuminen meni läpi ongelmitta, ja VPN-tunneli muodostui laitteiden välille.

Seuraavaksi ZyWALL 2 Plus -laitteeseen piti konfiguroida muutamia asetuksia, joita ei vielä voitu tehdä Lahdessa puutteellisten verkkotietojen takia.

Palomuurissa asiakkaalle tuli sallia pääsy tarkastelemaan prosessiverkon palvelimia omasta verkostaan, ja lisäksi palomuurissa tuli estää palvelinkoneiden pääsy internetiin. Asiakkaiden pääsy palvelinkoneisiin toteutettiin porttiohjauksien avulla. Asiakkaallehan näkyy vain ZyWALL 2 Plus -laitteen asiakkaan puoleisen liitännän IP-osoite eli WAN IP, joten kaikkien prosessiverkon laitteiden on löydyttävä samalla IP-osoitteella, vain osoitteen perässä oleva porttinumero muuttuu. Jos asiakkaan aliverkkona on 192.168.1.0/24 ja ZyWALL 2 Plus -laitteelle on määritelty IP-osoitteeksi 192.168.1.10, prosessiverkon palvelimet voivat löytyä esimerkiksi osoitteista 192.168.1.10:80, 192.168.1.10:8080 ja 192.168.1.10:8081.

Nyt ZyWALL 2 Plus oli konfiguroitu kuntoon, ja myös VPN-tunneli oli toiminnassa. Ukrainan tehtaan prosessiverkkoon saatiin Lahti Precision Oy:ltä yhteys SSL VPN -tunnelista, joten etäyhteysratkaisu toimi, kuten ideana oli. Ukraina oli tavallaan toinen pilottihanke, sillä siinä toteutettiin etäyhteys ensimmäisen kerran ZyWALL USG 300 -laitteen ja ZyWALL 2 Plus -laitteen välillä, ja käytössä oli myös SSL VPN -tunneli. Tämän hankkeen pohjalta on helpompi konfiguroida ja toteuttaa tulevia etäyhteyksiä, kun perusasiat ja mahdolliset ongelmat ovat tulleet selviksi.

4.10 Tuotteistaminen

Lopuksi etäyhteysratkaisu piti tuotteistaa. Tuotteistettuna tässä projektissa kehitetty etäyhteysratkaisu on helpompi toteuttaa ja myydä asiakkaalle. Tuotteistamisen ensimmäinen vaihe oli määritellä tarvittavat dokumentit ja vaiheet etäyhteysratkaisun toimittamiseen. Seuraavassa kuvattuna vaiheittain etäyhteysratkaisun toimittaminen ja vaiheisiin liittyvät dokumentit

1. Asiakkaalle lähetetään etäyhteyttä koskeva aineisto: tarjous, esite ja tekninen palvelukuvaus.
2. Salassapitosopimus allekirjoitetaan.

3. Asiakastietolomake ja laitoksen lähiverkon kuvaus täytetään (sisältää valitun ratkaisun, IP-osoitteet, protokollat, portit, palvelut, salasanat jne.).
4. Tarvittavat laitteet tilataan.
5. Laite konfiguroidaan konfigurointiohjeen mukaisesti.
6. Laite asennetaan ohjauskaappiin omassa kokoonpanossa tai asiakkaan luona, asennusohjeen mukaan.
7. VPN-yhteys testataan, testaus- ja käyttöönottopöytäkirja täytetään.
8. Etäkäyttö yleisen etäkäyttöohjeen sekä laitoksen lähiverkon kuvauksen mukaisesti.

Vaadittavia dokumentteja on siis yhdeksän kappaletta:

- tarjous
- esite
- tekninen palvelukuvaus
- salassapitosopimus
- asiakastietolomake ja laitoksen lähiverkon kuvaus
- konfigurointiohje
- asennusohje
- testaus- ja käyttöönottopöytäkirja
- etäkäyttöohje.

Dokumenteista ensimmäisenä lähdettiin suunnittelemaan ja tekemään esitettä ja teknistä palvelukuvausta. Nämä ovat tarjouksen yhteydessä ensimmäiset dokumentit, joita asiakkaille annetaan. Dokumenttien avulla saadaan selville asiakkaan kiinnostus yleisesti etäyhteysratkaisuun ja saadaan aikaiseksi vuoropuhelua etäyhteysratkaisuun liittyen. Dokumenttien tekoa varten tutustuttiin yleisesti tietoliikennealan esitteisiin ja teknisiin palvelukuvauksiin, joiden avulla osattiin soveltaa, mitä sisältöä näistä dokumenteista tulee löytyä. Sekä esitettä että teknistä palvelukuvausta varten pidettiin palaveri, jossa suunniteltiin dokumenttien sisältöä ja yleistä ulkoasua.

Esite on yhden sivun mittainen etäyhteysratkaisun esittely, jossa kerrotaan lyhyesti mikä VPN on, mitä hyötyä kustannusnäkökulmasta VPN tuo, etätuen tuomat mahdollisuudet, laajakaista- ja puhelinmodeemiyhteyksien erot, Lahti Precision Oy:n etäyhteysratkaisun pääosat sekä etäyhteysratkaisun tietoturvan taso. Teknisessä palvelukuvauksessa käydään tarkemmin läpi itse etäyhteysratkaisuun liittyviä asioita, sen ominaisuuksia sekä asennukseen ja toteuttamiseen liittyviä yksityiskohtia. Palvelukuvauksessa esitellään Lahti Precision Oy:n tarjoamat verkkotopologiaratkaisut etäyhteyttä varten: jokainen ratkaisu käydään läpi ja taulukoidaan vaadittavat laitteet ja palvelut sekä niiden toimittaja (Lahti Precision Oy / asiakas). Lisäksi käydään läpi yleisesti VPN-tekniikkaan liittyviä protokollia ja ominaisuuksia. Tulevaisuudessa tekniseen palvelukuvaukseen lisätään myös etätukipalvelun hinnat ja etätuen vasteajat.

Asiakastietolomake ja laitoksen lähiverkon kuvaus sisältää tiedot asiakkaasta sekä asiakkaan verkosta. Dokumentista käyvät ilmi asiakkaan valitsema verkkotopologiaratkaisu sekä yleiset tiedot yhteydestä. Lisäksi dokumentti sisältää listan Lahti Precision Oy:n prosessiverkon laitteista ja niiden IP-osoitteista sekä mahdolliset palvelut ja salasanat.

Konfigurointiohje tehtiin erikseen ZyWALL 2 Plus ja ZyWALL USG 300 -laitteille. Konfigurointiohje ei ole suora kopio valmistajan ohjekirjasta, vaan se sisältää etäyhteysratkaisua varten tehtävät konfiguraatiot. Konfigurointiohjeista käyvät ilmi mm. käytettävät salausasetukset ja autentikointimenetelmät sekä IP-osoitteiden ja reititystietojen asettamiset. Konfigurointiohjeet on tehty ottaen huomioon, että myös sellaiset henkilöt, joilla ei ole laajaa tietotaitoa VPN-tekniikoista ja tietoliikenteestä, osaavat konfiguroida laitteet itsenäisesti.

Kaikki tuotteistamisdokumentit eivät ole vielä opinnäytetyöprojektin tässä vaiheessa valmiita, tai niiden tekoa ei ole vielä aloitettu. Loput dokumentit valmistuvat, kun niiden tekoa varten saadaan tarvittavat tiedot ja niiden sisällöt käydään läpi.

5 YHTEENVETO

Tässä opinnäytetyössä suunniteltiin, toteutettiin ja tuotteistettiin etäyhteysratkaisu Lahti Precision Oy:lle. Etäyhteysratkaisun suunnitteluun käytettiin projektin kannalta tarpeeksi aikaa. Alkutilanteen hahmottaminen antoi hyvän pohjan uuden etäyhteysratkaisun toteutukselle, ja vaatimusten määrittely koettiin tärkeäksi hyvin suunnitellun etäyhteysratkaisun kannalta. Laitevertailuista ja -testeistä saatiin hyvin käytännön tietoa eri laitevalmistajien ratkaisuiden eroista ja voitiin valita parhaiten Lahti Precision Oy:n tarpeita vastaava etäyhteyslaitteisto.

Pilottihankkeen ja sitä seuraavan etäyhteyden toteutukset olivat tämän opinnäytetyöprojektin kulmakiviä. Näistä saatiin ensimmäiset käytännön kokemukset etäyhteysratkaisun toimivuudesta todellisuudessa testiympäristön ulkopuolella. Hankkeiden avulla saatiin selville mahdollisia vikatilanteita ja ratkaisut niihin, jotka puolestaan nopeuttavat tulevien etäyhteyksien toteutuksissa ilmenevien ongelmien ratkaisuja. Yleisimpiä ongelmia olivat pienet asetus- ja konfigurointivirheet VPN-päätelaitteissa. Ongelmat selvisivät tilanteissa nopeasti tutkimalla laitteiden lokitietoja. Hankkeiden etäyhteydet ovat myös olleet työntekijöiden käytössä, ja etäyhteysratkaisu on todettu suurimmilta osin toimivaksi. Tulevaisuudessa etäyhteysratkaisua kehitetään sen käytöstä saatujen kokemusten pohjalta.

Tuotteistaminen oli tärkeä osa-alue tässä opinnäytetyössä. Lahti Precision Oy:n on helpompi toteuttaa tuotteistettu etäyhteysratkaisu ja tulevaisuudessa tarjota ratkaisua asiakkaille. Tuotteistamisdokumenttien avulla etäyhteysratkaisu voidaan myös standardoida, jolloin tulevaisuudessa sen toteutukseen voidaan käyttää samoja menetelmiä kuin aikaisempiin ratkaisuihin.

Kokonaisuutena tämä opinnäytetyöprojekti onnistui sille asetetuissa tavoitteissa suunnitella, toteuttaa ja tuotteistaa etäyhteysratkaisu. Toimivan etäyhteysratkaisun avulla voidaan tulevaisuudessa toteuttaa myös muita palveluita monitoroinnin ja

vikatilanteiden selvityksen lisäksi. Lisäksi tuotteistettu etäyhteysratkaisu on yrityksen kannalta tärkeä, sitä on helpompi tarjota asiakkaalle. Tuotteistettu ratkaisu on myös testattu ja hyväksi todettu. Etäyhteysratkaisu maksaa itsensä nopeasti takaisin, kun asiantuntijainsinöörien matkustustarve vähenee. Tulevaisuudessa etäyhteysratkaisun käyttöaste kasvaa sitä mukaan, kun etäyhteyksiä toteutetaan uusiin asiakastehtaisiin.

Etäyhteydet ovat tärkeä osa-alue tietoliikenteen tulevaisuutta. Tulevaisuudessa etäyhteyksiä käytetään yhä enemmän mobiililaitteiden kautta. Etäyhteyksien ansiosta myös kiinteiden työpisteiden merkitys vähenee, minkä vuoksi myös yritysten toimitilojen tarve pienenee. Koska etäyhteydet vähentävät lisäksi työntekijöiden matkustustarvetta, ovat etäyhteydet ympäristöystävällinen ja vähän maapalloa kuormittava tietoliikenneratkaisu.

LÄHTEET

Aboba, B., Dixon, W. 2004. IPsec-Network Address Translation (NAT) Compatibility Requirements [viitattu: 27.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc3715.txt

Cisco Systems, Inc. 2006. Layer 2 Tunnel Protocol [viitattu 1.3.2009]. Saatavissa: http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm

Gleeson, B., Lin, A., Heinanen, J., Armitage, G. & Malis, A. 2000. A Framework for IP Based Virtual Private Networks [viitattu 27.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc2764.txt

Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. & Zorn, G. 1999 Point-to-Point Tunneling Protocol (PPTP)[viitattu 1.3.2009]. Saatavissa: http://www.ietf.org/rfc/rfc2637.txt

Harkins, D., Carrel, D. 1998. The Internet Key Exchange (IKE) [viitattu 28.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc2409.txt

Housley, R., Ford, W., Polk, W. & Solo, D. 1999. Internet X.509 Public Key Infrastructure [viitattu 28.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc2459.txt

Huttunen, A., Swander, B., Volpe, V., DiBurro, L. & Stenberg, M. 2005. UDP Encapsulation of IPsec ESP Packets [viitattu 27.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc3948.txt

Kent, S., Atkinson, R.1998. IP Authentication Header [viitattu: 26.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc2402.txt

Kent, S. 2005. IP Encapsulating Security Payload (ESP) [viitattu: 25.2.2009]. Saatavissa: http://www.ietf.org/rfc/rfc4303.txt

Mason, A. 2002. IPSec Overview Part Five: Security Associations. Cisco Press [viitattu 28.2.2009]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=25443

Microsoft 2003a. How VPN Works. [viitattu 1.3.2009]. Saatavissa: http://technet.microsoft.com/en-us/library/cc779919.aspx

Microsoft 2003b. What Is VPN? [viitattu 1.3.2009]. Saatavissa: http://technet.microsoft.com/en-us/library/cc739294.aspx

Microsoft 2009. Understanding PPTP (Windows NT 4.0) [viitattu 1.3.2009]. Saatavissa: http://technet.microsoft.com/en-us/library/cc768084.aspx

Perlmutter, B., Zarkower, J. 2001 Virtuaaliset yksityisverkot. Helsinki: Oy Edita Ab.

Salausmenetelmät 2008. [viitattu 1.3.2009]. Saatavissa: http://lipas.uwasa.fi/~h79423/ttp/ttp08.html

Scott, C., Wolfe, P. & Erwin, M. 1999. Virtual Private Networks. 2. painos. Sebastobol, CA: O'Reilly Media, Incorporated.

Techtarget 2009. What is SSL VPN? [viitattu 2.4.2009]. Saatavissa: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1201867,00.html#

Viestintävirasto 2007a. Salausmenetelmät. [viitattu 1.3.2009]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html

Viestintävirasto 2007b. Tiivistefunktiot [viitattu 1.3.2009]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/tiivistefunktiot.html

Viestintävirasto 2007c. VPN [viitattu 1.3.2009]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html

Wikipedia 2009a. IPsec [viitattu 27.2.2009]. Saatavissa: http://en.wikipedia.org/wiki/IPsec

Wikipedia 2009b. Layer 2 Tunneling Protocol [viitattu 1.3.2009]. Saatavissa: http://en.wikipedia.org/wiki/L2TP

Wikipedia 2009c. NAT traversal [viitattu 27.2.2009]. Saatavissa: http://en.wikipedia.org/wiki/NAT_traversal

Wikipedia 2009d. Point-to-point tunneling protocol [viitattu 1.3.2009]. Saatavissa: http://en.wikipedia.org/wiki/Point-to-point_tunneling_protocol

Wikipedia 2009e. SHA hash functions [viitattu 1.3.2009]. Saatavissa: http://en.wikipedia.org/wiki/SHA1

LIITTEET

	Siemens Scalance S612/S613	**Zyxel ZyWALL 2+**
VPN		
Protokolla	IPSec	IPSec
Salaus	DES, 3DES, AES	DES, 3DES, AES
Autentikointi		
paketti	MD5, SHA-1	MD5, SHA-1
käyttäjä	Pre-shared key (PSK), X.509	Pre-shared key (PSK), X.509
NAT-T	v	v
1:1 NAT		v
Dead Peer Detection	v	v
Hallinta	PC (Security Configuration Tool)	Web GUI (HTTP, HTTPS) CLI Vantage CNM
Käyttäjätunnukset	admin käyttäjä (rajoitetut oikeudet)	admin
Varayhteys		Dial Backup
Käyttölämpötila	0℃ - 60℃ (S612) -20℃ - 70℃ (S613)	0℃ - 50℃
Käyttöjännite	24V DC	12V DC
Hinta	S612 1032€ S613 1352€ Client 158€	138,80 €
Käyttöliittymä (www)	Security Configuration Tool helppokäyttöinen	Todella selkeä, hyvin jäsennelty, konfiguraatiovelhot
VPN-tunnelin luonti	moduulit ja SOFTNET Security Clientit samassa ryhmässä -> IPSec-tunneli muodostetaan automaattisesti (Scalance luo myös sertifikaatit itse), voidaan konfiguroida myös manuaalisesti, moduulit voivat kuulua useisiin eri ryhmiin	IP-osoitteet + muutamat asetukset ja tunneli on toimintakunnossa, sertifikaatit luodaan itse (esim. XCA) tai pyydetään esim VeriSign:ilta, myös konfiguraatiovelhot
VPN-tunnelin avaaminen/sulkeminen	aktiivi - aloittaa yhteyden passiivi - odottaa yhteyttä	Luodut VPN-tunnelit listassa, josta kuvaketta klikkaamalla avataan/suljetaan yhteys, vaatii admin oikeudet

Konfigurointidata	C-PLUG: konfiguraatiodata säilyy moduulin hajotessa, voidaan vaihtaa suoraan uuteen moduuliin	Backup & restore, konfigurointi tallennetaan koneelle
Loki	Loki: paikallinen, syslog	Loki: paikallinen, syslog
Ulkoiset ominaisuudet	Suunniteltu tehdaskäyttöön, hyvä kestävyys	Lähinnä toimistokäyttöön, vaatii jonkinlaisen asennus- ja suojaratkaisun
Muuta	GPRS-yhteys vaatii SINAUT GPRS router MD740-1 - reitittimen Ei vaadi muutoksia olemassa olevaan verkkoon Löytää automaattisesti sisäverkon laitteet	
Hylkäämisen syyt	ei 1:1 NAT ei voi kontrolloida tunnelien aukioloa kuin ottamalla piuhan irti hinta	

	Phoenix Contact FL mGuard RS VPN	**Hirschmann EAGLE mGuard TX/TX**
VPN		
Protokolla	IPSec, L2TP	IPSec, L2TP
Salaus	DES, 3DES, AES	DES, 3DES, AES
Autentikointi		
paketti	MD5, SHA-1	MD5, SHA-1
käyttäjä	Pre-shared key (PSK), X.509	Pre-shared key (PSK), X.509
NAT-T	v	v
1:1 NAT	v	v
Dead Peer Detection	v	v
Hallinta	Web GUI (HTTPS) SSH SNMPv1, v2, v3 V.24 (RS232)	Web GUI (HTTPS) CLI auto-configuration adapter SNMPv3 HiDiscovery Industrial HiVision
Käyttäjätunnukset	root admin	root admin
Varayhteys	Saatavilla modem/ISDN-mallit	
Käyttölämpötila	0℃ - 60℃	0℃ - 60℃
Käyttöjännite	redundanttinen 12V tai 24V DIN-kiskolle, IP20	redundanttinen 12V tai 24V DIN-kiskolle, IP20
Hinta	950 €	720 €
Käyttöliittymä (www)	Selkeä, hyvä värimaailma	Selkeä
VPN-tunnelin luonti	IP-osoitteet + muutamat asetukset ja tunneli on toimintakunnossa, sertifikaatit luodaan itse (esim. XCA)	IP-osoitteet + muutamat asetukset ja tunneli on toimintakunnossa, sertifikaatit luodaan itse (esim. XCA)

VPN-tunnelin avaaminen/sulkeminen	Luodut tunnelit listassa, josta voidaan avata/sulkea, vaatii admin oikeudet URL start/stop "VPN-nappi", yhteyden avaaminen ja sulkeminen nappia painamalla	Luodut tunnelit listassa, josta voidaan avata/sulkea, vaatii admin oikeudet URL start/stop
Konfigurointidata	Save & upload, konfigurointi tallennetaan koneelle	Save & upload, konfigurointi tallennetaan koneelle
Loki	Loki: paikallinen, syslog	Loki: paikallinen, syslog
Ulkoiset ominaisuudet	Suunniteltu tehdaskäyttöön	Suunniteltu tehdaskäyttöön
Muuta	Snapshot: pakattu tiedosto (tar.gz), jossa kaikki konfiguraatiotiedot ja lokitiedot	Snapshot: pakattu tiedosto (tar.gz), jossa kaikki konfiguraatiotiedot ja lokitiedot
Hylkäämisen syyt	hinta	hinta